CIS BIND 9.x STIG Benchmark

v1.0.0 - 09-11-2025

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (legalnotices@cisecurity.org) and request guidance on copyright usage.

NOTE: It is ***NEVER*** acceptable to host a CIS Benchmark in ***ANY*** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

Table of Contents

Terms of Use 1

Table of Contents 2

Overview 5

Target Technology Details 5

Intended Audience 5

Recommendation Definitions 6

Title 6

Assessment Status 6

Automated 6

Manual 6

Profile 6

Description 6

Rationale Statement 6

Audit Procedure 6

Remediation Procedure 7

Additional Information 7

Profile Definitions 8

Acknowledgements 9

Recommendations 10

1 STIG RULES 10

1.1 BIND-9X-001010 (Manual) 11

1.2 BIND-9X-001020 (Manual) 13

1.3 BIND-9X-001030 (Manual) 15

1.4 BIND-9X-001040 (Manual) 17

1.5 BIND-9X-001050 (Manual) 19

1.6 BIND-9X-001060 (Manual) 21

1.7 BIND-9X-001070 (Manual) 23

1.8 BIND-9X-001110 (Manual) 25

1.9 BIND-9X-001140 (Manual) 29

1.10 BIND-9X-001150 (Manual) 31

1.11 BIND-9X-001170 (Manual) 33

1.12 BIND-9X-001180 (Manual) 34

1.13 BIND-9X-001190 (Manual) 35

1.14 BIND-9X-001200 (Manual) 38

1.15 BIND-9X-001210 (Manual) 39

1.16 BIND-9X-001220 (Manual) 40

1.17 BIND-9X-001230 (Manual) 42

1.18 BIND-9X-001240 (Manual) 44

1.19 BIND-9X-001250 (Manual) 46

1.20 BIND-9X-001260 (Manual) 47

1.21 BIND-9X-001270 (Manual) 49
1.22 BIND-9X-001280 (Manual) 51
1.23 BIND-9X-001290 (Manual) 53
1.24 BIND-9X-001300 (Manual) 55
1.25 BIND-9X-001310 (Manual) 57
1.26 BIND-9X-001320 (Manual) 59
1.27 BIND-9X-001340 (Manual) 61
1.28 BIND-9X-001350 (Manual) 63
1.29 BIND-9X-001360 (Manual) 65
1.30 BIND-9X-001370 (Manual) 67
1.31 BIND-9X-001380 (Manual) 70
1.32 BIND-9X-001390 (Manual) 73
1.33 BIND-9X-001400 (Manual) 76
1.34 BIND-9X-001410 (Manual) 78
1.35 BIND-9X-001420 (Manual) 80
1.36 BIND-9X-001430 (Manual) 81
1.37 BIND-9X-001470 (Manual) 84
1.38 BIND-9X-001480 (Manual) 86
1.39 BIND-9X-001490 (Manual) 88
1.40 BIND-9X-001500 (Manual) 90
1.41 BIND-9X-001510 (Manual) 92
1.42 BIND-9X-001520 (Manual) 94
1.43 BIND-9X-001530 (Manual) 96
1.44 BIND-9X-001540 (Manual) 97
1.45 BIND-9X-001550 (Manual) 99
1.46 BIND-9X-001560 (Manual) 101
1.47 BIND-9X-001570 (Manual) 104
1.48 BIND-9X-001580 (Manual) 106
1.49 BIND-9X-001590 (Manual) 108
1.50 BIND-9X-001600 (Manual) 110
1.51 BIND-9X-001610 (Manual) 112
1.52 BIND-9X-001620 (Manual) 114
1.53 BIND-9X-001630 (Manual) 116
1.54 BIND-9X-001650 (Manual) 118
1.55 BIND-9X-001660 (Manual) 123
1.56 BIND-9X-001680 (Manual) 126
1.57 BIND-9X-001690 (Manual) 128
1.58 BIND-9X-001700 (Manual) 131
1.59 BIND-9X-001720 (Manual) 134
1.60 BIND-9X-001740 (Manual) 135
1.61 BIND-9X-001750 (Manual) 137
1.62 BIND-9X-001770 (Manual) 140
1.63 BIND-9X-001780 (Manual) 142
1.64 BIND-9X-001830 (Manual) 144
1.65 BIND-9X-001840 (Manual) 146
1.66 BIND-9X-001850 (Manual) 148
1.67 BIND-9X-001890 (Manual) 150
1.68 BIND-9X-001900 (Manual) 152
1.69 BIND-9X-001910 (Manual) 154
1.70 BIND-9X-001920 (Manual) 156
1.71 BIND-9X-001950 (Manual) 157
1.72 BIND-9X-002010 (Manual) 159
1.73 BIND-9X-002050 (Manual) 162

Appendix: Summary Table 164

Appendix: Change History 168

Overview

Target Technology Details

BIND 9.x Secure Technical Implementation Guide (STIG)

Version: 3 Release: 0.1 Benchmark

Date: 06 Mar 2025

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate BIND 9.x and are looking to comply with the STIG guidance

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted, or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations (or rules) for securing a technology or a supporting platform. STIG Benchmark profiles are used to identify which Vulnerability Severity Category Code (CAT) each rule is associated with.

Description

The Rule Title from the STIG.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Additional Information

References from the STIG Rule if applicable.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **SEVERITY: CAT I**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be high severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT II**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be medium severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT III**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be low severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

Acknowledgements

The Recommendations in this Benchmark are a representation of the Rules in the unclassified DISA STIG for BIND 9.x

Recommendations

1 STIG RULES

ISC BIND DNS 9.x

BIND 9.x Secure Technical Implementation Guide (STIG)

Version: 3 Release: 0.1 Benchmark

Date: 06 Mar 2025

CLASSIFICATION unclassified

1.1 BIND-9X-001010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

A BIND 9.x primary name server must limit the number of concurrent zone transfers between authorized secondary name servers.

```
GROUP ID: V-272364
RULE ID: SV-272364r1082285
```

Rationale:

Limiting the number of concurrent sessions reduces the risk of denial of service (DoS) to the DNS implementation.

Name servers do not have direct user connections but accept client connections for queries. Original restriction on client connections should be high enough to prevent a self-imposed DoS, after which the connections are monitored and fine-tuned to best meet the organization's specific requirements.

Primary name servers also make outbound connection to secondary name servers to provide zone transfers and accept inbound connection requests from clients wishing to provide a dynamic update. Primary name servers should explicitly limit zone transfers to only be made to designated secondary name servers. Because zone transfers involve the transfer of entire zones and use TCP connections, they place substantial demands on network resources relative to normal DNS queries. Errant or malicious frequent zone transfer requests on the name servers of the enterprise can overload the primary zone server and result in DoS to legitimate users. Primary name servers should be configured to limit the hosts from which they will accept dynamic updates.

Additionally, the number of concurrent clients, especially TCP clients, needs to be kept to a level that does not risk placing the system in a DoS state.

Audit:

If this is not a primary name server, this requirement is Not Applicable.

Verify that the name server is configured to limit the number of zone transfers from authorized secondary name servers.

Inspect the "named.conf" file for the following:

```
server <ip_address> {
transfers 2;
};
```

If each "server" statement does not contain a "transfers" substatement, this is a finding.

If the transfers value is greater than three this is a finding.

Remediation:

Edit the "named.conf" file.

Add the "transfers" substatement to each "server" statement block.

The value of the "transfers" option can be increased to a value no greater than three based on organizational requirements needed to support DNS operations.

Restart the BIND 9.x process.

Additional Information:

CCI-000054 Limit the number of concurrent sessions for each organization-defined account and/or account type to an organization-defined number.

- NIST SP 800-53::AC-10
- NIST SP 800-53A::AC-10.1 (ii)
- NIST SP 800-53 Revision 4::AC-10
- NIST SP 800-53 Revision 5::AC-10

1.2 BIND-9X-001020 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The BIND 9.x secondary name server must limit the number of zones requested from a single primary name server.

```
GROUP ID: V-272365
RULE ID: SV-272365r1067934
```

Rationale:

Limiting the number of concurrent sessions reduces the risk of denial of service (DoS) to the DNS implementation.

Name servers do not have direct user connections but accept client connections for queries. Original restriction on client connections should be high enough to prevent a self-imposed DoS, after which the connections are monitored and fine-tuned to best meet the organization's specific requirements.

Primary name servers also make outbound connection to secondary name servers to provide zone transfers and accept inbound connection requests from clients wishing to provide a dynamic update. Primary name servers should explicitly limit zone transfers to only be made to designated secondary name servers. Because zone transfers involve the transfer of entire zones and use TCP connections, they place substantial demands on network resources relative to normal DNS queries. Errant or malicious frequent zone transfer requests on the name servers of the enterprise can overload the primary zone server and result in DoS to legitimate users. Primary name servers should be configured to limit the hosts from which they will accept dynamic updates.

Additionally, the number of concurrent clients, especially TCP clients, needs to be kept to a level that does not risk placing the system in a DoS state.

Audit:

If this is not a secondary name server, this requirement is Not Applicable.

Verify that the secondary name server is configured to limit the number of zones requested from a single primary name server.

Inspect the "named.conf" file for the following:

```
options {
transfers-per-ns 2;
};
```

If the "options" statement does not contain a "transfers-per-ns" sub statement, this is a finding.

If the transfers-per-ns value is greater than three, this is a finding.

Remediation:

Edit the "named.conf" file.

Add the "transfers-per-ns" sub statement to the "options" statement block.

The value of the "transfers-per-ns" option can be increased to a value no greater than three based on organizational requirements needed to support DNS operations.

Restart the BIND 9.x process.

Additional Information:

CCI-000054 Limit the number of concurrent sessions for each organization-defined account and/or account type to an organization-defined number.

- NIST SP 800-53::AC-10
- NIST SP 800-53A::AC-10.1 (ii)
- NIST SP 800-53 Revision 4::AC-10
- NIST SP 800-53 Revision 5::AC-10

1.3 BIND-9X-001030 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The BIND 9.x secondary name server must limit the total number of zones the name server can request at any one time.

```
GROUP ID: V-272366
RULE ID: SV-272366r1082287
```

Rationale:

Limiting the number of concurrent sessions reduces the risk of denial of service (DoS) to the DNS implementation.

Name servers do not have direct user connections but accept client connections for queries. Original restriction on client connections should be high enough to prevent a self-imposed denial of service, after which the connections are monitored and fine-tuned to best meet the organization's specific requirements.

Primary name servers also make outbound connection to secondary name servers to provide zone transfers and accept inbound connection requests from clients wishing to provide a dynamic update. Primary name servers should explicitly limit zone transfers to only be made to designated secondary name servers. Because zone transfers involve the transfer of entire zones and use TCP connections, they place substantial demands on network resources relative to normal DNS queries. Errant or malicious frequent zone transfer requests on the name servers of the enterprise can overload the Primary zone server and result in DoS to legitimate users. Primary name servers should be configured to limit the hosts from which they will accept dynamic updates.

Additionally, the number of concurrent clients, especially TCP clients, needs to be kept to a level that does not risk placing the system in a DoS state.

Audit:

If this is not a secondary name server, this requirement is Not Applicable.

Verify the name server is configured to limit the total number of zones that can be requested at one time.

Inspect the "named.conf" file for the following:

```
options {
transfers-in 10;
};
```

If the "options" statement does not contain a "transfers-in" sub statement, this is a finding.

Remediation:

Edit the "named.conf" file.

Add the "transfers-in" substatement to the "options" statement block.

The value of the "transfers-in" will be based on organizational requirements needed to support DNS operations.

Restart the BIND 9.x process.

Additional Information:

CCI-000054 Limit the number of concurrent sessions for each organization-defined account and/or account type to an organization-defined number.

- NIST SP 800-53::AC-10
- NIST SP 800-53A::AC-10.1 (ii)
- NIST SP 800-53 Revision 4::AC-10
- NIST SP 800-53 Revision 5::AC-10

1.4 BIND-9X-001040 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The BIND 9.x server implementation must limit the number of concurrent session client connections to the number of allowed dynamic update clients.

```
GROUP ID: V-272367
RULE ID: SV-272367r1082290
```

Rationale:

Limiting the number of concurrent sessions reduces the risk of denial of service (DoS) to the DNS implementation.

Name servers do not have direct user connections but accept client connections for queries. Original restriction on client connections should be high enough to prevent a self-imposed denial of service, after which the connections are monitored and fine-tuned to best meet the organization's specific requirements.

Primary name servers also make outbound connections to secondary name servers to provide zone transfers and accept inbound connection requests from clients wishing to provide a dynamic update. Primary name servers should explicitly limit zone transfers to only be made to designated secondary name servers. Because zone transfers involve the transfer of entire zones and use TCP connections, they place substantial demands on network resources relative to normal DNS queries. Errant or malicious frequent zone transfer requests on the name servers of the enterprise can overload the primary zone server and result in DoS to legitimate users. Primary name servers should be configured to limit the hosts from which they will accept dynamic updates.

Additionally the number of concurrent clients, especially TCP clients, needs to be kept to a level that does not risk placing the system in a DoS state.

Audit:

Verify the name server is configured to limit the number of concurrent client connections to the number of allowed dynamic update clients.

Inspect the "named.conf" file for the following:

```
options {
transfers-out 10;
};
```

If the "options" statement does not contain a "transfers-out" substatement, this is a finding.

Remediation:

Edit the "named.conf" file.

Add the "transfers-out" substatement to the "options" statement block.

The value of the "transfers-out" will be based on organizational requirements needed to support DNS operations.

Restart the BIND 9.x process.

Additional Information:

CCI-000054 Limit the number of concurrent sessions for each organization-defined account and/or account type to an organization-defined number.

- NIST SP 800-53::AC-10
- NIST SP 800-53A::AC-10.1 (ii)
- NIST SP 800-53 Revision 4::AC-10
- NIST SP 800-53 Revision 5::AC-10

1.5 BIND-9X-001050 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The print-severity variable for the configuration of BIND 9.x server logs must be configured to produce audit records containing information to establish what type of events occurred.

```
GROUP ID: V-272368
RULE ID: SV-272368r1082293
```

Rationale:

Auditing and logging are key components of any security architecture. It is essential for security personnel to know what is being performed on the system, where an event occurred, when an event occurred, and by whom the event was triggered, to compile an accurate risk assessment. Logging the actions of specific events provides a means to investigate an attack, recognize resource utilization or capacity thresholds, or to simply identify an improperly configured DNS implementation. Without log records that aid in the establishment of what types of events occurred and when those events occurred, there is no traceability for forensic or analytical purposes, and the cause of events is severely hindered.

Audit:

For each logging channel that is defined, verify that the "print-severity" substatement is listed.

Inspect the "named.conf" file for the following:

```
logging {
channel channel_name {
print-severity yes;
};
};
```

If the "print-severity" statement is missing, this is a finding.

If the "print-severity" statement is not set to "yes", this is a finding.

Remediation:

Edit the "named.conf" file.

Add the "print-severity" substatement to the "channel" statement.

Configure the "print-severity" sub statement to "yes".

Restart the BIND 9.x process.

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

1.6 BIND-9X-001060 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The print-time variable for the configuration of BIND 9.x server logs must be configured to establish when (date and time) the events occurred.

```
GROUP ID: V-272369
RULE ID: SV-272369r1082296
```

Rationale:

Without establishing when events occurred, it is impossible to establish, correlate, and investigate the events relating to an incident.

Associating event types with detected events in the application and audit logs provides a means of investigating an attack, recognizing resource utilization or capacity thresholds, or identifying an improperly configured application. To compile an accurate risk assessment and provide forensic analysis, it is essential for security personnel to know when events occurred (date and time).

Audit:

For each logging channel that is defined, verify that the "print-time" substatement is listed.

Inspect the "named.conf" file for the following:

```
logging {
channel channel_name {
print-time yes;
};
};
```

If the "print-time" statement is missing, this is a finding.

If the "print-time" statement is not set to "yes", this is a finding.

Remediation:

Edit the "named.conf" file.

Add the "print-time" substatement to the "channel" statement.

Configure the "print-time" sub statement to "yes".

Restart the BIND 9.x process.

Additional Information:

CCI-000131 Ensure that audit records containing information that establishes when the event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 b

1.7 BIND-9X-001070 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The print-category variable for the configuration of BIND 9.x server logs must be configured to record information indicating which process generated the events.

```
GROUP ID: V-272370
RULE ID: SV-272370r1067949
```

Rationale:

Without establishing where events occurred, it is impossible to establish, correlate, and investigate the events relating to an incident. Associating information about where the event occurred within the application provides a means of investigating an attack, recognizing resource utilization or capacity thresholds, or identifying an improperly configured application. To compile an accurate risk assessment and provide forensic analysis, it is essential for security personnel to know where events occurred, such as application components, modules, session identifiers, filenames, host names, and functionality.

Audit:

For each logging channel that is defined, verify that the "print-category" sub statement is listed.

Inspect the "named.conf" file for the following:

```
logging {
channel channel_name {
print-category yes;
};
};
```

If the "print-category" statement is missing, this is a finding.

If the "print-category" statement is not set to "yes", this is a finding.

Remediation:

Edit the "named.conf" file.

Add the "print-category" sub statement to the "channel" statement.

Configure the "print-category" sub statement to "yes".

Restart the BIND 9.x process.

Additional Information:

CCI-000132 Ensure that audit records containing information that establishes where the event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 c

1.8 BIND-9X-001110 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

A BIND 9.x server implementation must be configured to allow DNS administrators to audit all DNS server components based on selectable event criteria; and produce audit records within all DNS server components that contain information for failed security verification tests, information to establish the outcome and source of the events, any information necessary to determine cause of failure, and any information necessary to return to operations with least disruption to mission processes.

```
GROUP ID: V-272371
RULE ID: SV-272371r1082239
```

Rationale:

Without the capability to generate audit records, it would be difficult to establish, correlate, and investigate the events relating to an incident, or identify those responsible for one. The actual auditing is performed by the OS/NDM, but the configuration to trigger the auditing is controlled by the DNS server.

The list of audited events is the set of events for which audits are to be generated. This set of events is typically a subset of the list of all events for which the system is capable of generating audit records.

The DOD has defined the list of events for which the application will provide an audit record generation capability as the following:

(i) Successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g., classification levels);

(ii) Access actions, such as successful and unsuccessful logon attempts, privileged activities or other system-level access, starting and ending time for user access to the system, concurrent logons from different workstations, successful and unsuccessful accesses to objects, all program initiations, and all direct access to the information system; and

(iii) All account creation, modification, disabling, and termination actions.

The DOD has defined the data which the application will provide an audit record generation capability for an event as the following:

(i) Establish the source of the event;

(ii) The outcome of the event; and

(iii) Identify the application itself as the source of the event.

Without establishing the source of the event, it is impossible to establish, correlate, and investigate the events leading up to an outage or attack. Associating information about the source of the event within the application provides a means of investigating an attack, recognizing resource utilization or capacity thresholds, or identifying an improperly configured application.

Without information about the outcome of events, security personnel cannot make an accurate assessment about whether an attack was successful or if changes were made to the security state of the system.

Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the information system after the event occurred). As such, they also provide a means to measure the impact of an event and help authorized personnel to determine the appropriate response.

Failure to a known state can address safety or security in accordance with the mission/business needs of the organization. Failure to a known secure state helps prevent a loss of confidentiality, integrity, or availability in the event of a failure of the information system or a component of the system. Preserving application state information helps to facilitate application restart and return to the operational mode of the organization with less disruption to mission-essential processes.

The DNS server should be configured to generate audit records whenever a self-test fails. The OS/NDM is responsible for generating notification messages related to this audit record.

If authorized individuals do not have the ability to modify auditing parameters in response to a changing threat environment, the organization may not be able to effectively respond, and important forensic information may be lost.

This requirement enables organizations to extend or limit auditing as necessary to meet organizational requirements. Auditing that is limited to conserve information system resources may be extended to address certain threat situations. In addition, auditing may be limited to a specific set of events to facilitate audit reduction, analysis, and reporting. Organizations can establish time thresholds in which audit actions are changed, for example, near real-time, within minutes, or within hours.

In addition to logging where events occur within the application, the application must also produce audit records that identify the application itself as the source of the event. To compile an accurate risk assessment and provide forensic analysis, it is essential for security personnel to know the source of the event, particularly in the case of centralized logging. In the case of centralized logging, the source would be the application name accompanied by the host or client name.

Satisfies: SRG-APP-000089-DNS-000004, SRG-APP-000098-DNS-000009, SRG-APP-000099-DNS-000010, SRG-APP-000275-DNS-000040, SRG-APP-000226-DNS-000032

Audit:

Verify the name server is configured to generate audit records.

Inspect the "named.conf" file for the following:

```
logging {
channel channel_name {
severity info;
};
category default { channel_name; };
};
```

If there is no "logging" statement, this is a finding.

If the "logging" statement does not contain a "channel", this is a finding.

If the "logging" statement does not contain a "category" that uses a "channel", this is a finding.

Remediation:

Configure the logging statement in the "named.conf" file:

```
logging {
channel <channel_name> {
file "<file_name>";
severity info;
};
category default { <channel_name>; };
};
```

Replace <channel_name> and <file_name> with names that distinctively identify the purpose of the channel and the log file.

Restart the BIND 9.x process.

Additional Information:

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

CCI-000133 Ensure that audit records containing information that establishes the source of the event.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 d

CCI-000134 Ensure that audit records containing information that establishes the outcome of the event.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 e

CCI-001294 Alert organization-defined personnel or roles of failed security verification tests.

- NIST SP 800-53::SI-6 (1)
- NIST SP 800-53A::SI-6 (1).1
- NIST SP 800-53 Revision 4::SI-6 c
- NIST SP 800-53 Revision 5::SI-6 c

CCI-001665 Preserve organization-defined system state information in the event of a system failure.

- NIST SP 800-53::SC-24
- NIST SP 800-53A::SC-24.1 (v)
- NIST SP 800-53 Revision 4::SC-24
- NIST SP 800-53 Revision 5::SC-24

1.9 BIND-9X-001140 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The BIND 9.x server private key corresponding to the zone-signing key (ZSK) pair must be the only DNSSEC key kept on a name server that supports dynamic updates.

```
GROUP ID: V-272372
RULE ID: SV-272372r1082241
```

Rationale:

The private key in the ZSK key pair must be protected from unauthorized access. If possible, the private key should be stored offline (with respect to the internet-facing, DNSSEC-aware name server) in a physically secure, nonnetwork-accessible machine along with the zone file primary copy.

This strategy is not feasible in situations in which the DNSSEC-aware name server has to support dynamic updates. To support dynamic update transactions, the DNSSEC-aware name server (which usually is a primary authoritative name server) has to have both the zone file primary copy and the private key corresponding to the zone-signing key (ZSK-private) online to immediately update the signatures for the updated RRsets.

Failure to protect the private ZSK opens it to being maliciously obtained and opens the DNS zone to being populated with invalid data. The integrity of the DNS zone would be compromised, leading to a loss of trust whether a DNS response has originated from an authentic source, the response is complete and has not been tampered with during transit.

Audit:

Determine if the BIND 9.x server is configured to allow dynamic updates.

Review the "named.conf" file for any instance of the "allow-update" statement. The following example disables dynamic updates:

```
allow-update {none;};
```

If the BIND 9.x implementation is not configured to allow dynamic updates, verify with the system administrator (SA) that the ZSK private key is stored offline. If it is not, this is a finding.

If the BIND 9.x implementation is configured to allow dynamic updates, verify that the ZSK private key is the only key stored on the name server.

For each signed zone file, identify the ZSK "key id" number:

```
# cat <signed_zone_file> | grep -i "zsk"
ZSK; alg = ECDSAP256SHA256; key id = 22335
```

Using the ZSK "key id", verify that the only private key stored on the system matches the "key id":

```
Kexample.com.+008+22335.private
```

If any ZSK private keys exist on the server other than the one corresponding to the active ZSK pair, this is a finding.

Remediation:

Remove any ZSK private keys existing on the server other than the one corresponding to the active ZSK pair.

Additional Information:

CCI-000186 For public key-based authentication, enforce authorized access to the corresponding private key.

- NIST SP 800-53::IA-5 (2)
- NIST SP 800-53A::IA-5 (2).1
- NIST SP 800-53 Revision 4::IA-5 (2) (b)
- NIST SP 800-53 Revision 5::IA-5 (2) (a) (1)

1.10 BIND-9X-001150 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The BIND 9.x server signature generation using the key signing key (KSK) must be done off-line, using the KSK-private key stored offline.

```
GROUP ID: V-272373
RULE ID: SV-272373r1082243
```

Rationale:

The private key in the KSK key pair must be protected from unauthorized access. The private key should be stored offline (with respect to the internet-facing, DNSSEC-aware name server) in a physically secure, nonnetwork-accessible machine along with the zone file primary copy.

Failure to protect the private KSK may have significant effects on the overall security of the DNS infrastructure. A compromised KSK could lead to an inability to detect unauthorized DNS zone data resulting in network traffic being redirected to a rogue site.

Audit:

Ensure no private KSKs are stored on the name sever.

With the assistance of the DNS administrator, obtain a list of all DNSSEC private keys that are stored on the name server.

Inspect the signed zone files(s) and if there are local zones, look for the KSK key ID:

```
DNSKEY 257 3 8 ( <hash_algorithm) ; KSK ; alg = ECDSAP256SHA256; key id =
52807
```

Verify that none of the identified private keys are KSKs.

An example private KSK would look like the following:

```
Kexample.com.+008+52807.private
```

If private KSKs are stored on the name server, this is a finding.

Remediation:

Remove all private KSKs from the name server and ensure that they are stored offline in a secure location.

Additional Information:

CCI-000186 For public key-based authentication, enforce authorized access to the corresponding private key.

- NIST SP 800-53::IA-5 (2)
- NIST SP 800-53A::IA-5 (2).1
- NIST SP 800-53 Revision 4::IA-5 (2) (b)
- NIST SP 800-53 Revision 5::IA-5 (2) (a) (1)

1.11 BIND-9X-001170 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The key file used by a BIND 9.x server must be owned by the account under which the name server software is run.

```
GROUP ID: V-272374
RULE ID: SV-272374r1082245
```

Rationale:

To enable zone transfer (requests and responses) through authenticated messages, it is necessary to generate a key for every pair of name servers. The key can also be used for securing other transactions, such as dynamic updates, DNS queries, and responses. The binary key string that is generated by most key generation utilities used with DNSSEC is Base64 encoded. TSIG is a string used to generate the message authentication hash stored in a TSIG RR and used to authenticate an entire DNS message.

Audit:

Verify permissions assigned to the TSIG keys enforce read-write access to the key owner and deny access to group or system users.

With the assistance of the DNS administrator, determine the location of the TSIG keys used by the BIND 9.x implementation:

```
# ls -al <TSIG_Key_Location>
-rw-------. 1 named named 76 May 10 20:35 tsig-example.key
```

If the key files are more permissive than 600, this is a finding.

Remediation:

Change the permissions of the TSIG key files:

```
# chmod 600 <TSIG_key_file>
```

Additional Information:

CCI-000186 For public key-based authentication, enforce authorized access to the corresponding private key.

- NIST SP 800-53::IA-5 (2)
- NIST SP 800-53A::IA-5 (2).1
- NIST SP 800-53 Revision 4::IA-5 (2) (b)
- NIST SP 800-53 Revision 5::IA-5 (2) (a) (1)

1.12 BIND-9X-001180 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The read and write access to a TSIG key file used by a BIND 9.x server must be restricted to only the account that runs the name server software.

```
GROUP ID: V-272375
RULE ID: SV-272375r1082247
```

Rationale:

Weak permissions of a TSIG key file could allow an adversary to modify the file, thus defeating the security objective.

Audit:

Verify permissions assigned to the TSIG keys enforce read-write access to the key owner and deny access to group or system users.

With the assistance of the DNS administrator, determine the location of the TSIG keys used by the BIND 9.x implementation:

```
# ls -al <TSIG_Key_Location>
-rw-------. 1 named named 76 May 10 20:35 tsig-example.key
```

If the key files are more permissive than 600, this is a finding.

Remediation:

Change the permissions of the TSIG key files:

```
# chmod 600 <TSIG_key_file>
```

Additional Information:

CCI-000186 For public key-based authentication, enforce authorized access to the corresponding private key.

- NIST SP 800-53::IA-5 (2)
- NIST SP 800-53A::IA-5 (2).1
- NIST SP 800-53 Revision 4::IA-5 (2) (b)
- NIST SP 800-53 Revision 5::IA-5 (2) (a) (1)

1.13 BIND-9X-001190 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

A unique TSIG key used by a BIND 9.x server must be generated for each pair of communicating hosts.

```
GROUP ID: V-272376
RULE ID: SV-272376r1067967
```

Rationale:

To enable zone transfer (requests and responses) through authenticated messages, it is necessary to generate a key for every pair of name servers. The key also can be used for securing other transactions, such as dynamic updates, DNS queries, and responses. The binary key string that is generated by most key generation utilities used with DNSSEC is Base64 encoded. TSIG is a string used to generate the message authentication hash stored in a TSIG RR and used to authenticate an entire DNS message.

The process of authenticating the source of a message and its integrity through hash-based message authentication codes (HMAC) is specified through a set of DNS specifications known collectively as TSIG. The sender of the message uses the HMAC function to generate a MAC and sends this MAC along with the message to the receiver. The receiver, who shares the same secret key, uses the key and HMAC function used by the sender to compute the MAC on the received message. The receiver then compares the computed MAC with the received MAC; if the two values match, it provides assurance that the message has been received correctly and that the sender belongs to the community of users sharing the same secret key. Thus, message source authentication and integrity verification are performed in a single process. To enable zone transfer (requests and responses) through authenticated messages, it is necessary to generate a key for every pair of name servers. The key also can be used for securing other transactions, such as dynamic updates, DNS queries, and responses. The binary key string that is generated by most key generation utilities used with DNSSEC is Base64 encoded. TSIG is a string used to generate the message authentication hash stored in a TSIG RR and used to authenticate an entire DNS message.

Audit:

Verify that the BIND 9.x server is configured to use separate TSIG key-pairs when securing server-to-server transactions.

Inspect the "named.conf" file for the presence of TSIG key statements:

On the primary name server, this is an example of a configured key statement:

```
key tsig_example. {
algorithm hmac-SHA1;
include "tsig-example.key";
};

zone "disa.mil" {
type Primary;
file "db.disa.mil";
allow-transfer { key tsig_example.; };
};
```

On the secondary name server, this is an example of a configured key statement:

```
key tsig_example. {
algorithm hmac-SHA1;
include "tsig-example.key";
};

server <ip_address> {
keys { tsig_example };
};

zone "disa.mil" {
type Secondary;
Primarys { <ip_address>; };
file "db.disa.mil";
};
```

Verify that each TSIG key-pair listed is only used by a single key statement:

```
# cat <tsig_key_file>
```

If any TSIG key-pair is being used by more than one key statement, this is a finding.

Remediation:

Create a separate TSIG key-pair for each key statement listed in the named.conf file.

Configure the name server to use separate TSIG key-pairs for each key statement listed in the named.conf file.

Restart the BIND 9.x process.

Additional Information:

CCI-000186 For public key-based authentication, enforce authorized access to the corresponding private key.

- NIST SP 800-53::IA-5 (2)
- NIST SP 800-53A::IA-5 (2).1
- NIST SP 800-53 Revision 4::IA-5 (2) (b)
- NIST SP 800-53 Revision 5::IA-5 (2) (a) (1)

1.14 BIND-9X-001200 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The TSIG keys used with the BIND 9.x implementation must be owned by a privileged account.

```
GROUP ID: V-272377
RULE ID: SV-272377r1067970
```

Rationale:

Incorrect ownership of a TSIG key file could allow an adversary to modify the file, thus defeating the security objective.

Audit:

With the assistance of the DNS administrator, identify all of the TSIG keys used by the BIND 9.x implementation.

Identify the account that the "named" process is running as:

```
# ps -ef | grep named
named 3015 1 0 12:59 ? 00:00:00 /usr/sbin/named -u named -t /var/named/chroot
```

With the assistance of the DNS administrator, determine the location of the TSIG keys used by the BIND 9.x implementation.

```
# ls -al <TSIG_Key_Location>
-rw-------. 1 named named 76 May 10 20:35 tsig-example.key
```

If any of the TSIG keys are not owned by the above account, this is a finding.

Remediation:

Change the ownership of the TSIG keys to the named process it is running as.

```
# chown <named_proccess_owner> <TSIG_key_file>.
```

Additional Information:

CCI-000186 For public key-based authentication, enforce authorized access to the corresponding private key.

- NIST SP 800-53::IA-5 (2)
- NIST SP 800-53A::IA-5 (2).1
- NIST SP 800-53 Revision 4::IA-5 (2) (b)
- NIST SP 800-53 Revision 5::IA-5 (2) (a) (1)

1.15 BIND-9X-001210 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The TSIG keys used with the BIND 9.x implementation must be group owned by a privileged account.

```
GROUP ID: V-272378
RULE ID: SV-272378r1067973
```

Rationale:

Incorrect ownership of a TSIG key file could allow an adversary to modify the file, thus defeating the security objective.

Audit:

With the assistance of the DNS administrator, identify all of the TSIG keys used by the BIND 9.x implementation.

Identify the account that the "named" process is running as:

```
# ps -ef | grep named
named 3015 1 0 12:59 ? 00:00:00 /usr/sbin/named -u named -t /var/named/chroot
```

With the assistance of the DNS administrator, determine the location of the TSIG keys used by the BIND 9.x implementation.

```
# ls -al <TSIG_Key_Location>
-rw-------. 1 named named 76 May 10 20:35 tsig-example.key
```

If any of the TSIG keys are not group owned by the above account, this is a finding.

Remediation:

Change the group ownership of the TSIG keys to the named process group.

```
# chgrp <named_proccess_group> <TSIG_key_file>
```

Additional Information:

CCI-000186 For public key-based authentication, enforce authorized access to the corresponding private key.

- NIST SP 800-53::IA-5 (2)
- NIST SP 800-53A::IA-5 (2).1
- NIST SP 800-53 Revision 4::IA-5 (2) (b)
- NIST SP 800-53 Revision 5::IA-5 (2) (a) (1)

1.16 BIND-9X-001220 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

On a BIND 9.x server for zones split between the external and internal sides of a network, the RRs for the external hosts must be separate from the RRs for the internal hosts.

```
GROUP ID: V-272379
RULE ID: SV-272379r1067976
```

Rationale:

Authoritative name servers for an enterprise may be configured to receive requests from both external and internal clients.

External clients need to receive RRs that pertain only to public services (public web server, mail server, etc.).

Internal clients need to receive RRs pertaining to public services as well as internal hosts.

The zone information that serves the RRs on both the inside and the outside of a firewall should be split into different physical files for these two types of clients (one file for external clients and one file for internal clients).

Audit:

If the BIND 9.x name server is not configured for split DNS, this is Not Applicable.

Verify that the BIND 9.x server is configured to use separate views and address space for internal and external DNS operations when operating in a split configuration.

Inspect the "named.conf" file for the following:

```
view "internal" {
match-clients { <ip_address> | <address_match_list> };
zone "example.com" {
type Primary;
file "internals.example.com";
};
};
view "external" {
match-clients { <ip_address> | <address_match_list> };
zone "example.com" {
type Primary;
file "externals.db.example.com";
allow-transfer { Secondarys; };
};
};
```

If the internal and external view statements are configured to use the same zone file, this is a finding.

Inspect the zone file defined in the internal and external view statements.

If any resource record is listed in both the internal and external zone files, this is a finding.

Remediation:

Edit the "named.conf" file.

Configure the internal and external view statements to use separate zone files.

Edit the internal and external zone files.

Configure the zone file to use RRs designated for internal or external use. The zone files should not share any RR.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.17 BIND-9X-001230 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

On a BIND 9.x server in a split DNS configuration, where separate name servers are used between the external and internal networks, the internal name server must be configured to not be reachable from outside resolvers.

```
GROUP ID: V-272380
RULE ID: SV-272380r1082248
```

Rationale:

Instead of having the same set of authoritative name servers serve different types of clients, an enterprise could have two different sets of authoritative name servers.

One set, called external name servers, can be located within a DMZ. These would be the only name servers that are accessible to external clients and would serve RRs pertaining to hosts with public services (web servers that serve external web pages or provide B2C services, mail servers, etc.).

The other set, called internal name servers, must be located within the firewall. They should be configured so they are not reachable from outside and therefore provide naming services exclusively to internal clients.

Audit:

If the BIND 9.x name server is not configured for split DNS, this is Not Applicable.

Verify that the BIND 9.x server is configured to use the "match-clients" sub statement to limit the reach of the internal view from the external view.

Inspect the "named.conf" file for the following:

```
view "internal" {
match-clients { <ip_address> | <address_match_list>; };
};
```

If the "match-clients" sub statement is missing for the internal view, this is a finding.

If the "match-clients" sub statement for the internal view does not limit the view to authorized hosts, this is a finding.

If any of the IP addresses defined for the "match-clients" substatement in the internal view are assigned to external hosts, this is a finding.

Remediation:

Edit the "named.conf" file.

Configure the internal view statement to limit use authorized internal hosts:

```
view "internal" {
match-clients { <ip_address> | <address_match_list>; };
};
```

Remove any IP address that is assigned to an external host from the internal view statement.

Restart the BIND 9.x process.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.18 BIND-9X-001240 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

On a BIND 9.x server in a split DNS configuration, where separate name servers are used between the external and internal networks, the external name server must be configured to not be reachable from inside resolvers.

```
GROUP ID: V-272381
RULE ID: SV-272381r1068944
```

Rationale:

Instead of having the same set of authoritative name servers serve different types of clients, an enterprise could have two different sets of authoritative name servers.

One set, called external name servers, can be located within a DMZ; these would be the only name servers that are accessible to external clients and would serve RRs pertaining to hosts with public services (web servers that serve external web pages or provide B2C services, mail servers, etc.)

The other set, called internal name servers, is to be located within the firewall and should be configured so they are not reachable from outside and hence provide naming services exclusively to internal clients.

Audit:

If the BIND 9.x name server is not configured for split DNS, this is Not Applicable.

Verify that the external view of the BIND 9.x server is configured to only serve external hosts.

Inspect the "named.conf" file for the following:

```
view "external" {
match-clients { <ip_address> | <address_match_list>; };
};
```

If the "match-clients" substatement does not limit the external view to external hosts only, this is a finding.

Remediation:

Edit the "named.conf" file.

Configure the external view statement to server external hosts only:

```
view "external" {
match-clients { <ip_address> | <address_match_list>; };
};
```

Restart the BIND 9.x process.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.19 BIND-9X-001250 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

A BIND 9.x implementation operating in a split DNS configuration must be approved by the organization's authorizing official (AO).

```
GROUP ID: V-272382
RULE ID: SV-272382r1068269
```

Rationale:

BIND 9.x has implemented an option to use "view" statements to allow for split DNS architecture to be configured on a single name server.

If the split DNS architecture is improperly configured, there is a risk that internal IP addresses and host names could leak into the external view of the DNS server.

Allowing private IP space to leak into the public DNS system may provide a person with malicious intent the ability to footprint the network and identify potential attack targets residing on the private network.

Audit:

If the BIND 9.x name server is not configured for split DNS, this is Not Applicable.

Verify that the split DNS implementation has been approved by the organizations AO.

With the assistance of the DNS administrator, obtain the AO's letter of approval for the split DNS implementation.

If the split DNS implementation has not been approved by the organizations AO, this is a finding.

Remediation:

Obtain approval for the split DNS implementation from the AO.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.20 BIND-9X-001260 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

On the BIND 9.x server the IP address for hidden primary authoritative name servers must not appear in the name servers set in the zone database.

```
GROUP ID: V-272383
RULE ID: SV-272383r1067988
```

Rationale:

A hidden primary authoritative server is an authoritative DNS server whose IP address does not appear in the name server set for a zone. All of the name servers that do appear in the zone database as designated name servers get their zone data from the hidden primary via a zone transfer request. In effect, all visible name servers are actually secondary servers. This prevents potential attackers from targeting the primary name server because its IP address may not appear in the zone database.

Audit:

If the BIND 9.x name server is not configured for split DNS, this is Not Applicable.

With the assistance of the DNS administrator, identify if the BIND 9.x implementation is using a hidden primary name server. If it is not, this is Not Applicable.

In a split DNS configuration that is using a hidden primary name server, verify that the name server IP address is not listed in the zone file.

With the assistance of the DNS administrator, obtain the IP address of the hidden primary name server.

Inspect each zone file used by the hidden primary name server and its secondary zones.

If the IP address for the hidden primary name server is listed in any of the zone files, this is a finding.

Remediation:

Edit the zone file(s).

Remove all references to the hidden primary name server.

Restart the BIND 9.x process.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.21 BIND-9X-001270 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

A BIND 9.x server NSEC3 must be used for all internal DNS zones.

```
GROUP ID: V-272384
RULE ID: SV-272384r1068270
```

Rationale:

To ensure that RRs associated with a query are really missing in a zone file and have not been removed in transit, the DNSSEC mechanism provides a means for authenticating the nonexistence of an RR. It generates a special RR called an NSEC (or NSEC3) RR that lists the RRTypes associated with an owner name as well as the next name in the zone file. It sends this special RR, along with its signatures, to the resolving name server. By verifying the signature, a DNSSEC-aware resolving name server can determine which authoritative owner name exists in a zone and which authoritative RRTypes exist at those owner names.

Audit:

If the server is on an internal, restricted network with reserved IP space, this is Not Applicable.

With the assistance of the DNS administrator, identify each internal DNS zone listed in the "named.conf" file.

For each internal zone identified, inspect the signed zone file for the NSEC resource records:

```
86400 NSEC example.com. A RRSIG NSEC
```

If the zone file does not contain an NSEC record for the zone, this is a finding.

Remediation:

Re-sign each zone that is missing NSEC records.

Restart the BIND 9.x process.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.22 BIND-9X-001280 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

On the BIND 9.x server the private keys corresponding to both the zone signing key (ZSK) and the key signing key (KSK) must not be kept on the BIND 9.x DNSSEC-aware primary authoritative name server when the name server does not support dynamic updates.

```
GROUP ID: V-272385
RULE ID: SV-272385r1067994
```

Rationale:

The private keys in the KSK and ZSK key pairs must be protected from unauthorized access. If possible, the private keys should be stored offline (with respect to the internet-facing, DNSSEC-aware name server) in a physically secure, nonnetwork-accessible machine along with the zone file primary copy.

This strategy is not feasible in situations in which the DNSSEC-aware name server has to support dynamic updates. To support dynamic update transactions, the DNSSEC-aware name server (which usually is a primary authoritative name server) has to have both the zone file primary copy and the private key corresponding to the zone-signing key (ZSK-private) online to immediately update the signatures for the updated RRsets. The private key corresponding to the key-signing key (KSK-private) can still be kept offline.

Audit:

Determine if the BIND 9.x server is configured to allow dynamic updates.

Review the "named.conf" file for any instance of the "allow-update" statement. The following example disables dynamic updates:

```
allow-update {none;};
```

If the BIND 9.x implementation is not configured to allow dynamic updates, verify with the system administrator (SA) that the private ZSKs and private KSKs are stored offline. If not, this is a finding.

Remediation:

Remove any ZSK or KSK private key from any BIND 9.x server that does not support dynamic updates.

Note: Any ZSK or KSK that is not needed to support dynamic updates should be stored offline in a secure location.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.23 BIND-9X-001290 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The two files generated by the BIND 9.x server dnssec-keygen program must be owned by the root account or deleted once they have been copied to the key file in the name server.

```
GROUP ID: V-272386
RULE ID: SV-272386r1082250
```

Rationale:

To enable zone transfer (requests and responses) through authenticated messages, it is necessary to generate a key for every pair of name servers. The key also can be used for securing other transactions, such as dynamic updates, DNS queries, and responses. The binary key string that is generated by most key generation utilities used with DNSSEC is Base64 encoded. A TSIG is a string used to generate the message authentication hash stored in a TSIG RR and used to authenticate an entire DNS message.

Audit:

With the assistance of the DNS administrator, identify all dnssec-keygen key files that reside on the BIND 9.x server.

An example dnssec-keygen key file will look like the following:

`Kns1.example.com_ns2.example.com.+161+28823.key`

OR

`Kns1.example.com_ns2.example.com.+161+28823.private`

For each key file identified, verify that the key file is owned by "root":

```
# ls -al
-r-------- 1 root root 77 Jul 1 15:00
Kns1.example.com_ns2.example.com+161+28823.key
```

If the key file(s) are not owned by root, this is a finding.

Remediation:

Change the ownership of the keys to the root account.

```
# chown root <key_file>.
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.24 BIND-9X-001300 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The two files generated by the BIND 9.x server dnssec-keygen program must be group owned by the server administrator account or deleted once they have been copied to the key file in the name server.

```
GROUP ID: V-272387
RULE ID: SV-272387r1082252
```

Rationale:

To enable zone transfer (requests and responses) through authenticated messages, it is necessary to generate a key for every pair of name servers. The key also can be used for securing other transactions such as dynamic updates, DNS queries, and responses. The binary key string that is generated by most key generation utilities used with DNSSEC is Base64 encoded. A TSIG is a string used to generate the message authentication hash stored in a TSIG RR and used to authenticate an entire DNS message.

Audit:

With the assistance of the DNS administrator, identify all dnssec-keygen key files that reside on the BIND 9.x server.

An example dnssec-keygen key file will look like the following:

`Kns1.example.com_ns2.example.com.+161+28823.key`

OR

`Kns1.example.com_ns2.example.com.+161+28823.private`

For each key file identified, verify that the key file is owned by "root":

```
# ls -al
-r-------- 1 root root 77 Jul 1 15:00
Kns1.example.com_ns2.example.com+161+28823.key
```

If the key file(s) are not owned by root, this is a finding.

Remediation:

Change the group ownership of the keys to the root group.

```
# chgrp root <key_file>.
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.25 BIND-9X-001310 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Permissions assigned to the dnssec-keygen keys used with the BIND 9.x implementation must enforce read-only access to the key owner and deny access to all other users.

```
GROUP ID: V-272388
RULE ID: SV-272388r1082254
```

Rationale:

To enable zone transfer (requests and responses) through authenticated messages, it is necessary to generate a key for every pair of name servers. The key also can be used for securing other transactions such as dynamic updates, DNS queries, and responses. The binary key string that is generated by most key generation utilities used with DNSSEC is Base64 encoded. A TSIG is a string used to generate the message authentication hash stored in a TSIG RR and used to authenticate an entire DNS message. Weak permissions could allow an adversary to modify the file(s), thus defeating the security objective.

Audit:

With the assistance of the DNS administrator, identify all dnssec-keygen key files that reside on the BIND 9.x server.

An example dnssec-keygen key file will look like the following:

`Kns1.example.com_ns2.example.com.+161+28823.key`

OR

`Kns1.example.com_ns2.example.com.+161+28823.private`

For each key file identified, verify that the key file is owned by "root":

```
# ls -al
-r-------- 1 root root 77 Jul 1 15:00
Kns1.example.com_ns2.example.com+161+28823.key
```

If the key file(s) are not owned by root, this is a finding.

Remediation:

Change the permissions of the dnssec-keygen key files:

```
# chmod 400 <key_file>
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.26 BIND-9X-001320 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

A BIND 9.x server validity period for the RRSIGs covering a zones DNSKEY RRSet must be no less than two days and no more than one week.

```
GROUP ID: V-272389
RULE ID: SV-272389r1068006
```

Rationale:

The best way for a zone administrator to minimize the impact of a key compromise is by limiting the validity period of RRSIGs in the zone and in the parent zone. This strategy limits the time during which an attacker can take advantage of a compromised key to forge responses. An attacker that has compromised a zone signing key (ZSK) can use that key only during the key signing key's (KSK's) signature validity interval. An attacker that has compromised a KSK can use that key for only as long as the signature interval of the RRSIG covering the DS RR in the delegating parent. These validity periods should be short, which will require frequent re-signing.

Audit:

With the assistance of the DNS administrator, identify the RRSIGs that cover the DNSKEY resource record set for each zone.

Each record will list an expiration and inception date, the difference of which will provide the validity period.

The dates are listed in the following format:

YYYYMMDDHHMMSS

For each RRSIG identified, verify that the validity period is no less than two days and is no longer than seven days.

If the validity period is outside of the specified range, this is a finding.

Remediation:

Re-sign each zone that is outside of the validity period.

Restart the BIND 9.x process.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.27 BIND-9X-001340 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

On the BIND 9.x server the private key corresponding to the zone signing key (ZSK), stored on name servers accepting dynamic updates, must be owned by root.

```
GROUP ID: V-272390
RULE ID: SV-272390r1068009
```

Rationale:

The private keys in the key signing key (KSK) and ZSK key pairs must be protected from unauthorized access. If possible, the private keys should be stored offline (with respect to the internet-facing, DNSSEC-aware name server) in a physically secure, nonnetwork-accessible machine along with the zone file primary copy.

This strategy is not feasible in situations in which the DNSSEC-aware name server has to support dynamic updates. To support dynamic update transactions, the DNSSEC-aware name server (which usually is a primary authoritative name server) has to have both the zone file primary copy and the private key corresponding to the zone-signing key (ZSK-private) online to immediately update the signatures for the updated RRsets. The private key corresponding to the key-signing key (KSK-private) can still be kept offline.

Audit:

Note: This check only verifies for ZSK key file ownership. Permissions for key files are required under BIND-9X-001132 and BIND-9X-001142.

For each signed zone file, identify the ZSK "key id" number:

```
# cat <signed_zone_file> | grep -i "zsk"
ZSK; alg = ECDSAP256SHA256; key id = 22335
```

Using the ZSK "key id", identify the private ZSK.

```
Kexample.com.+008+22335.private
```

Verify that the private ZSK is owned by root:

```
# ls -l <ZSK_key_file>
-r------- 1 root root 1776 Jul 3 17:56 Kexample.com.+008+22335.private
```

If the key file is not owned by root, this is a finding.

Remediation:

Change the ownership of the ZSK private key to the root account.

```
# chown root <key_file>
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.28 BIND-9X-001350 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

On the BIND 9.x server the private key corresponding to the zone signing key (ZSK), stored on name servers accepting dynamic updates, must be group owned by root.

```
GROUP ID: V-272391
RULE ID: SV-272391r1068271
```

Rationale:

The private keys in the key signing key (KSK) and ZSK key pairs must be protected from unauthorized access. If possible, the private keys should be stored offline (with respect to the internet-facing, DNSSEC-aware name server) in a physically secure, nonnetwork-accessible machine along with the zone file primary copy.

This strategy is not feasible in situations in which the DNSSEC-aware name server has to support dynamic updates. To support dynamic update transactions, the DNSSEC-aware name server (which usually is a primary authoritative name server) has to have both the zone file primary copy and the private key corresponding to the zone-signing key (ZSK-private) online to immediately update the signatures for the updated RRsets. The private key corresponding to the key-signing key (KSK-private) can still be kept offline.

Audit:

Note: This check only verifies for ZSK key file ownership. Permissions for key files are required under BIND-9X-001132 and BIND-9X-001142.

For each signed zone file, identify the ZSK "key id" number:

```
# cat <signed_zone_file> | grep -i "zsk"
ZSK; alg = ECDSAP256SHA256; key id = 22335
```

Using the ZSK "key id", verify the private ZSK.

```
Kexample.com.+008+22335.private
```

Verify that the private ZSK is owned by root:

```
# ls -l <ZSK_key_file>
-r------- 1 root root 1776 Jul 3 17:56 Kexample.com.+008+22335.private
```

If the key file is not group owned by root, this is a finding.

Remediation:

Change the group ownership of the ZSK private key to the root group account.

```
# chgrp root <key_file>
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.29 BIND-9X-001360 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The BIND 9.x server implementation must prohibit the forwarding of queries to servers controlled by organizations outside of the U.S. government.

```
GROUP ID: V-272392
RULE ID: SV-272392r1068015
```

Rationale:

If remote servers to which DOD DNS servers send queries are controlled by entities outside of the U.S. government the possibility of a DNS attack is increased.

The Enterprise Recursive Service (ERS) provides the ability to apply enterprise-wide policy to all recursive DNS traffic that traverses the NIPRNet-to-Internet boundary. All recursive DNS servers on the NIPRNet must be configured to exclusively forward DNS traffic traversing NIPRNet-to-Internet boundary to the ERS anycast IPs.

Organizations need to carefully configure any forwarding that is being used by their caching name servers. They should only configure "forwarding of all queries" to servers within the DOD. Systems configured to use domain-based forwarding should not forward queries for mission critical domains to any servers that are not under the control of the U.S. government.

Audit:

If the server is not a caching server, this is Not Applicable.

This is Not Applicable to SIPR.

Note: The use of the Defense Research and Engineering Network (DREN) Enterprise Recursive DNS servers, as mandated by the DODIN service provider DREN, meets the intent of this requirement.

Verify that the server is configured to forward all DNS traffic to the DISA ERS anycast IP addresses (<IP_ADDRESS_LIST>;):

Inspect the "named.conf" file for the following:

```
forward only;
forwarders { <IP_ADDRESS_LIST>; };
```

If the "named.conf" options are not set to forward queries only to the ERS anycast IPs, this is a finding.

Note: "<IP_ADDRESS_LIST>" should be replaced with the current ERS IP addresses.

Remediation:

Configure the BIND 9.x caching name server to use the DISA ERS anycast IP addresses.

Edit the "named.conf" file and add the following to the global options statement:

```
forward only;
forwarders { <IP_ADDRESS_LIST>; };
```

Note: "<IP_ADDRESS_LIST>" should be replaced with the current ERS IP addresses.

Restart the BIND 9.x process.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.30 BIND-9X-001370 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The secondary name servers in a BIND 9.x implementation must be configured to initiate zone update notifications to other authoritative zone name servers.

```
GROUP ID: V-272393
RULE ID: SV-272393r1082256
```

Rationale:

It is important to maintain the integrity of a zone file. The serial number of the SOA record is used to indicate to secondary name server that a change to the zone has occurred and a zone transfer should be performed. The serial number used in the SOA record provides the DNS administrator a method to verify the integrity of the zone file based on the serial number of the last update and ensure that all Secondary servers are using the correct zone file.

When a primary name server notices that the serial number of a zone has changed, it sends a special announcement to all of the Secondary name servers for that zone. The primary name server determines which servers are the Secondarys for the zone by looking at the list of NS records in the zone and taking out the record that points to the name server listed in the MNAME field of the zone's SOA record as well as the domain name of the local host.

When a secondary name server receives a NOTIFY announcement for a zone from one of its configured Primary name servers, it responds with a NOTIFY response. The response tells the primary that the secondary received the NOTIFY announcement so that the primary can stop sending it NOTIFY announcements for the zone. Then the secondary proceeds just as if the refresh timer for that zone had expired: it queries the primary name server for the SOA record for the zone that the primary claims has changed. If the serial number is higher, the secondary transfers the zone.

The secondary should next issue its own NOTIFY announcements to the other authoritative name servers for the zone. The idea is that the primary may not be able to notify all of the secondary name servers for the zone itself, since it's possible some secondaries cannot communicate directly with the primary (they use another secondary as their primary). Older BIND 8 secondaries do not send NOTIFY messages unless explicitly configured to do so.

Audit:

If this is a primary name server, this is Not Applicable.

On a secondary name server, verify that the global notify is disabled. The global entry for the name server is under the "Options" section and notify should be disabled at this section.

Inspect the "named.conf" file for the following:

```
options {
notify no;
};
```

If the "notify" statement is missing, this is a finding.

If the "notify" statement is set to "yes", this is a finding.

Verify that zones for which the secondary server is authoritative is configured to notify other authorized secondary name servers when a zone file update has been received from the primary name server for the zone. Each zone has its own zone section.

Inspect the "named.conf" file for the following:

```
zone example.com {
notify explicit;
also-notify { <ip_address>; | <address_match_list>; };
```

If an "address match list" is used, verify that each IP address listed is an authorized secondary name server for that zone.

If the "notify explicit" statement is missing, this is a finding.

If the "also-notify" statement is missing, this is a finding.

If the "also-notify" statement is configured to notify name servers that are not authorized for that zone, this is a finding.

Remediation:

Edit the "named.conf" file.

Configure the "notify" sub statement in the "options" statement block to "no":

```
options {
notify no;
};
```

Configure the "notify explicit" and "also-notify" substatements in the zone statement block to limit zone transfer notifications to authorized secondary name servers:

```
zone example.com {
notify explicit;
also-notify { <ip_address>; | <address_match_list>; };
```

Restart the BIND 9.x process.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.31 BIND-9X-001380 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

A BIND 9.x server implementation must prohibit recursion on authoritative name servers.

```
GROUP ID: V-272394
RULE ID: SV-272394r1068272
```

Rationale:

A potential vulnerability of DNS is that an attacker can poison a name server's cache by sending queries that will cause the server to obtain host-to-IP address mappings from bogus name servers that respond with incorrect information. Once a name server has been poisoned, legitimate clients may be directed to nonexistent hosts (which constitutes a denial of service), or worse, hosts that masquerade as legitimate ones to obtain sensitive data or passwords.

To guard against poisoning, name servers authoritative for .mil domains should be separated functionally from name servers that resolve queries on behalf of internal clients. Organizations may achieve this separation by dedicating machines to each function or, if possible, by running two instances of the name server software on the same machine: one for the authoritative function and the other for the resolving function. In this design, each name server process may be bound to a different IP address or network interface to implement the required segregation.

DNSSEC ensures that the answer received when querying for name resolution actually comes from a trusted name server. Since DNSSEC is still far from being globally deployed external to DOD, and many resolvers either have not been updated or do not support DNSSEC, maintaining cached zone data separate from authoritative zone data mitigates the gap until all DNS data is validated with DNSSEC.

Since DNS forwarding of queries can be accomplished in some DNS applications without caching locally, DNS forwarding is the method to be used when providing external DNS resolution to internal clients.

Satisfies: SRG-APP-000383-DNS-000047, SRG-APP-000246-DNS-000035

Audit:

If this is a recursive name server, this is Not Applicable.

Note: A recursive name server should NOT be configured as an authoritative name server for any zone.

Verify that the BIND 9.x server is configured to prohibit recursion on authoritative name servers.

Inspect the "named.conf" file for the following:

```
options {
recursion no;
allow-recursion {none;};
allow-query {none;};
};
```

If the "recursion" sub statement is missing, or set to "yes", this is a finding.

If the "allow-recursion" sub statement is missing or is not set to "none", this is a finding.

If the "allow-query" sub statement under the "options statement" is missing or is not set to "none", this is a finding.

Verify that an "allow-query" sub statement under each zone statement is configured to authorized hosts:

```
zone "example.com" {
type Primary;
file "db.example.com";
allow-query { (address_match_list | <ip_address>) };
};
```

If the "allow-query" sub statement under each zone statement is not restricted to authorized hosts, this is a finding.

Remediation:

Configure the authoritative name server to prohibit recursion.

Edit the "named.conf" file and add the following sub statements to the options statement:

```
recursion no;
allow-recursion {none;};
allow-query { none };
```

Configure each zone to limit queries to authorized hosts:

Edit the "named.conf" file and add the following sub statement to each zone definition:

```
allow-query { address_match_list; };
```

Restart the BIND 9.x process.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

CCI-001094 Restrict the ability of individuals to launch organization-defined denial of service attacks against other systems.

- NIST SP 800-53::SC-5 (1)
- NIST SP 800-53A::SC-5 (1).1
- NIST SP 800-53 Revision 4::SC-5 (1)
- NIST SP 800-53 Revision 5::SC-5 (1)

1.32 BIND-9X-001390 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The primary servers in a BIND 9.x implementation must notify authorized secondary name servers when zone files are updated.

```
GROUP ID: V-272395
RULE ID: SV-272395r1082259
```

Rationale:

It is important to maintain the integrity of a zone file. The serial number of the SOA record is used to indicate to secondary name server that a change to the zone has occurred and a zone transfer should be performed. The serial number used in the SOA record provides the DNS administrator a method to verify the integrity of the zone file based on the serial number of the last update and ensure that all Secondary servers are using the correct zone file.

When a primary name server notices that the serial number of a zone has changed, it sends a special announcement to all of the secondary name servers for that zone. The primary name server determines which servers are the secondaries for the zone by looking at the list of NS records in the zone and taking out the record that points to the name server listed in the MNAME field of the zone's SOA record as well as the domain name of the local host.

When a secondary name server receives a NOTIFY announcement for a zone from one of its configured primary name servers, it responds with a NOTIFY response. The response tells the primary that the secondary received the NOTIFY announcement so that the primary can stop sending it NOTIFY announcements for the zone. Then the secondary proceeds just as if the refresh timer for that zone had expired: it queries the primary name server for the SOA record for the zone that the primary claims has changed. If the serial number is higher, the secondary transfers the zone.

The secondary should issue its own NOTIFY announcements to the other authoritative name servers for the zone. The idea is that the primary may not be able to notify all of the secondary name servers for the zone itself, since it is possible some secondaries cannot communicate directly with the primary (they use another secondary as their primary). Older BIND 8 Secondarys don't send NOTIFY messages unless explicitly configured to do so.

Audit:

If this is a secondary name server, this is Not Applicable.

On a primary name server, verify that the global notify is disabled. The global entry for the name server is under the "Options" section and "notify" should be disabled at this section.

Inspect the "named.conf" file for the following:

```
options {
notify no;
};
```

If the "notify" statement is missing, this is a finding.

If the "notify" statement is set to "yes", this is a finding.

Verify that each zone is configured to notify authorized secondary name servers when a zone file has been updated. Each zone has its own zone section.

Inspect the "named.conf" file for the following:

```
zone example.com {
notify explicit;
also-notify { <ip_address>; | <address_match_list>; };
```

If an "address match list" is used, verify that each IP address listed is an authorized secondary name server for that zone.

If the "notify explicit" statement is missing, this is a finding.

If the "also-notify" statement is missing, this is a finding.

If the "also-notify" statement is configured to notify name servers that are not authorized for that zone, this is a finding.

Remediation:

Edit the "named.conf" file.

Configure the "notify" sub statement in the "options" statement block to "no":

```
options {
notify no;
};
```

Configure the "notify explicit" and "also-notify" sub statements in the zone statement block to limit zone transfer notifications to authorized secondary name servers:

```
zone example.com {
notify explicit;
also-notify { <ip_address>; | <address_match_list>; };
```

Restart the BIND 9.x process.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.33 BIND-9X-001400 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

On a BIND 9.x server all root name servers listed in the local root zone file hosted on a BIND 9.x authoritative name server must be valid for that zone.

```
GROUP ID: V-272396
RULE ID: SV-272396r1068027
```

Rationale:

All caching name servers must be authoritative for the root zone because, without this starting point, they would have no knowledge of the DNS infrastructure and thus would be unable to respond to any queries. The security risk is that an adversary could change the root hints and direct the caching name server to a bogus root server. At that point, every query response from that name server is suspect, which would give the adversary substantial control over the network communication of the name servers' clients.

Audit:

If this is an authoritative name server, this is Not Applicable.

Identify the local root zone file in named.conf:

```
zone "." IN {
type hint;
file "<file_name>"
};
```

Examine the local root zone file.

If the local root zone file lists domains outside of the name server's primary domain, this is a finding.

Remediation:

Edit the local root zone file.

Remove any reference to a domain that is outside of the name server's primary domain.

Restart the BIND 9.x process.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.34 BIND-9X-001410 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

On a BIND 9.x server all root name servers listed in the local root zone file hosted on a BIND 9.x authoritative name server must be empty or removed.

```
GROUP ID: V-272397
RULE ID: SV-272397r1068030
```

Rationale:

A potential vulnerability of DNS is that an attacker can poison a name server's cache by sending queries that will cause the server to obtain host-to-IP address mappings from bogus name servers that respond with incorrect information. The DNS architecture needs to maintain one name server whose zone records are correct and the cache is not poisoned. In this effort, the authoritative name server may not forward queries; one of the ways to prevent this is to delete the root hints file.

When authoritative servers are sent queries for zones that they are not authoritative for and they are configured as a noncaching server (as recommended), they can either be configured to return a referral to the root servers or to refuse to answer the query. The requirement is to configure authoritative servers to refuse to answer queries for any zones for which they are not authoritative. This is more efficient for the server and allows it to spend more of its resources for its intended purpose of answering authoritatively for its zone.

Audit:

If this server is a caching name server, this is Not Applicable.

Ensure there is not a local root zone on the name server.

Inspect the "named.conf" file for the following:

```
zone "." IN {
type hint;
file "<file_name>"
};
```

If the file name identified is not empty or does exist, this is a finding.

Remediation:

Remove the local root zone file from the name server.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.35 BIND-9X-001420 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The BIND 9.x authoritative name servers must be configured to only receive zone transfer requests from specified secondary name servers.

```
GROUP ID: V-272398
RULE ID: SV-272398r1068033
```

Rationale:

Authoritative name servers (especially primary name servers) should be configured with an allow-transfer access control substatement designating the list of hosts from which zone transfer requests can be accepted. These restrictions address the denial-of-service threat and potential exploits from unrestricted dissemination of information about internal resources. Based on the need to know, the only name servers that need to refresh their zone files periodically are the secondary name servers. Zone transfer from primary name servers should be restricted to secondary name servers. The zone transfer should be completely disabled in the secondary name servers. The address match list argument for the allow-transfer substatement should consist of IP addresses of secondary name servers and stealth secondary name servers.

Audit:

Inspect the "named.conf" file for the following:

```
allow-transfer {
<ip>;
<ip2>;
};
```

If there is an "allow-transfer" statement, the IP's listed must be servers authorized to request transfers or this is a finding.

Remediation:

Remove unauthorized servers from the allow-transfer IP list in the "named.conf" file.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.36 BIND-9X-001430 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The BIND 9.x server implementation must implement internal/external role separation.

```
GROUP ID: V-272399
RULE ID: SV-272399r1068274
```

Rationale:

DNS servers with an internal role only process name/address resolution requests from within the organization (i.e., internal clients). DNS servers with an external role only process name/address resolution information requests from clients external to the organization (i.e., on the external networks, including the internet). The set of clients that can access an authoritative DNS server in a particular role is specified by the organization using address ranges, explicit access control lists, etc. To protect internal DNS resource information, it is important to isolate the requests to internal DNS servers.

Failure to separate internal and external roles in DNS may lead to address space that is private (e.g., 10.0.0.0/24) or is otherwise concealed by some form of Network Address Translation from leaking into the public DNS system. Allowing private IP space to leak into the public DNS system may provide a person with malicious intent the ability to footprint the network and identify potential attack targets residing on the private network.

Audit:

Severity override guidance: If the internal and external views are on separate network segments, this finding may be downgraded to a CAT II.

If the BIND 9.x name server is not configured for split DNS, this is Not Applicable.

Verify that the BIND 9.x server is configured to use separate views and address space for internal and external DNS operations when operating in a split configuration.

Inspect the "named.conf" file for the following:

```
view "internal" {
match-clients { <ip_address> | <address_match_list> };
zone "example.com" {
type Primary;
file "internals.example.com";
};
};
view "external" {
match-clients { <ip_address> | <address_match_list> };
zone "example.com" {
type Primary;
file "externals.db.example.com";
allow-transfer { Secondarys; };
};
};
```

If an external view is listed before an internal view, this is a finding.

If the internal and external views are on the same network segment, this is a finding.

Note: BIND 9.x reads the "named.conf" file from top to bottom. If a less stringent "match-clients" statement is processed before a more stringent "match-clients" statement, the more stringent statement will be ignored. With this in mind, all internal view statements should be listed before any external view statement in the "named.conf" file.

Remediation:

Edit the "named.conf" file.

Configure the internal and external view statements to use separate network segments.

Configure all internal view statements to be listed before any external view statement.

Restart the BIND 9.x process.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.37 BIND-9X-001470 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Every NS record in a zone file on a BIND 9.x server must point to an active name server and that name server must be authoritative for the domain specified in that record.

```
GROUP ID: V-272400
RULE ID: SV-272400r1082262
```

Rationale:

Poorly constructed NS records pose a security risk because they create conditions under which an adversary might be able to provide the missing authoritative name services that are improperly specified in the zone file. The adversary could issue bogus responses to queries that clients would accept because they learned of the adversary's name server from a valid authoritative name server, one that need not be compromised for this attack to be successful. The list of secondary servers must remain current within 72 hours of any changes to the zone architecture that would affect the list of secondaries. If a Secondary server has been retired or is not operational but remains on the list, then an adversary might have a greater opportunity to impersonate that secondary without detection, rather than if the secondary were actually online. For example, the adversary may be able to spoof the retired secondary's IP address without an IP address conflict, which would not be likely to occur if the true secondary were active.

Audit:

Verify that each name server listed on the BIND 9.x server is authoritative for the domain it supports.

Inspect the "named.conf" file and identify all of the zone files that the BIND 9.x server is using.

```
zone "example.com" {
file "zone_file";
};
```

Inspect each zone file and identify each NS record listed.

```
86400 NS ns1.example.com
86400 NS ns2.example.com
```

With the assistance of the DNS administrator, verify that each name server listed is authoritative for that domain.

If name servers are listed in the zone file that are not authoritative for the specified domain, this is a finding.

Remediation:

Edit the zone file(s).

Remove any name server for which the BIND 9.x server is not authoritative.

Restart the BIND 9.x process.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.38 BIND-9X-001480 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

On a BIND 9.x server all authoritative name servers for a zone must be located on different network segments.

```
GROUP ID: V-272401
RULE ID: SV-272401r1082264
```

Rationale:

Most enterprises have an authoritative primary server and a host of authoritative secondary name servers. It is essential that these authoritative name servers for an enterprise be located on different network segments. This dispersion ensures the availability of an authoritative name server not only in situations in which a particular router or switch fails but also during events involving an attack on an entire network segment.

Audit:

Verify that each name server listed on the BIND 9.x server is on a separate network segment.

Inspect the "named.conf" file and identify all of the zone files that the BIND 9.x server is using.

```
zone "example.com" {
file "zone_file";
};
```

Inspect each zone file and identify each A record for each NS record listed:

```
ns1.example.com 86400 IN A 192.168.1.4
ns2.example.com 86400 IN A 192.168.2.4
```

If name servers are listed in the zone file that are not on different network segments for the specified domain, this is a finding.

Remediation:

Edit the zone file and configure each name server on a separate network segment.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.39 BIND-9X-001490 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

On the BIND 9.x server the platform on which the name server software is hosted must be configured to send outgoing DNS messages from a random port.

```
GROUP ID: V-272402
RULE ID: SV-272402r1068045
```

Rationale:

OS configuration practices as issued by the U.S. Computer Emergency Response Team (US CERT) and the National Institute of Standards and Technology's (NIST's) National Vulnerability Database (NVD), based on identified vulnerabilities that pertain to the application profile into which the name server software fits should be always followed. In particular, hosts that run the name server software should not provide any other services and therefore should be configured to respond to DNS traffic only. In other words, the only allowed incoming ports/protocols to these hosts should be 53/udp and 53/tcp.

Outgoing DNS messages should be sent from a random port to minimize the risk of an attacker guessing the outgoing message port and sending forged replies.

Audit:

Verify that the BIND 9.x server does not limit outgoing DNS messages to a specific port.

Inspect the "named.conf" file for the any instance of the "port" flag:

```
options {
listen-on port 53 { <ip_address>; };
listen-on-v6 port 53 { <ip_v6_address>; };
};
```

If any "port" flag is found outside of the "listen-on" or "listen-on-v6" statements, this is a finding.

Remediation:

Edit the "named.conf" file.

Configure the BIND 9.x server to only use the "port" flag with the "listen-on" and "listen-on-v6" statements:

```
options {
listen-on port 53 { <ip_address>; };
listen-on-v6 port 53 { <ip_v6_address>; };
};
```

Restart the BIND 9.x process.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.40 BIND-9X-001500 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

A BIND 9.x server implementation must be operating on a Current-Stable version as defined by ISC.

```
GROUP ID: V-272403
RULE ID: SV-272403r1068048
```

Rationale:

Each newer version of the name server software, especially the BIND software, generally is devoid of vulnerabilities found in earlier versions because it has design changes incorporated to take care of those vulnerabilities. These vulnerabilities have been exploited (i.e., some form of attack was launched), and sufficient information has been generated with respect to the nature of those exploits. It makes good business sense to run the latest version of name server software because theoretically it is the safest version. Even if the software is the latest version, it is not safe to run it in default mode. The security administrator should always configure the software to run in the recommended secure mode of operation after becoming familiar with the new security settings for the latest version.

Audit:

Verify that the BIND 9.x server is at a version that is considered "Current-Stable" by ISC or latest supported version of BIND when BIND is installed as part of a specific vendor implementation where the vendor maintains the BIND patches.

```
# named -v
```

The above command should produce a version number similar to the following:

```
BIND 9.9.4-RedHat-9.9.4-29.el7_2.3
```

If the server is running a version that is not listed as "Current-Stable" by ISC, this is a finding.

Remediation:

Update the BIND 9.x server to a version that is listed as "Current-Stable" by ISC or the latest supported version of BIND when BIND is installed as part of a specific vendor implementation where the vendor maintains the BIND patches.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.41 BIND-9X-001510 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The host running a BIND 9.x implementation must use a dedicated management interface to separate management traffic from DNS specific traffic.

```
GROUP ID: V-272404
RULE ID: SV-272404r1068051
```

Rationale:

Providing Out-Of-Band (OOB) management is the best first step in any management strategy. No production traffic resides on an out-of-band network. The biggest advantage to implementation of an OOB network is providing support and maintenance to the network that has become degraded or compromised. During an outage or degradation period the in-band management link may not be available.

Audit:

Verify that the BIND 9.x server is configured to use a dedicated management interface:

```
# ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.0.1.252 netmask 255.255.255.0 broadcast 10.0.1.255
inet6 fd80::21c:d8ff:fab7:1dba prefixlen 64 scopeid 0x20<link>
ether 00:1a:b8:d7:1a:bf txqueuelen 1000 (Ethernet)
RX packets 2295379 bytes 220126493 (209.9 MiB)
RX errors 0 dropped 31 overruns 0 frame 0
TX packets 70507 bytes 12284940 (11.7 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1458
inet 10.0.0.5 netmask 255.255.255.0 broadcast 10.0.0.255
inet6 fe81::21c:a8bf:fad7:1dca prefixlen 64 scopeid 0x20<link>
ether 00:1d:d8:b5:1c:dd txqueuelen 1000 (Ethernet)
RX packets 39090 bytes 4196802 (4.0 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 93250 bytes 18614094 (17.7 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

If one of the interfaces listed is not dedicated to only process management traffic, this is a finding.

Remediation:

On the host machine, configure an interface that is dedicated to management traffic.

Restart the host machine.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.42 BIND-9X-001520 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The host running a BIND 9.x implementation must use an interface that is configured to process only DNS traffic.

```
GROUP ID: V-272405
RULE ID: SV-272405r1068054
```

Rationale:

Configuring hosts that run a BIND 9.x implementation to only accept DNS traffic on a DNS interface allows a system to be configured to segregate DNS traffic from all other host traffic.

The TCP/IP stack in DNS hosts (stub resolver, caching/resolving/recursive name server, authoritative name server, etc.) could be subjected to packet flooding attacks (such as SYNC and smurf), resulting in disruption of communication.

The use of a dedicated interface for DNS traffic allows for these threats to be mitigated by creating a means to limit what types of traffic can be processed using a host-based firewall solution.

Audit:

Verify that the BIND 9.x server is configured to use an interface that is configured to process only DNS traffic.

```
# ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.0.1.252 netmask 255.255.255.0 broadcast 10.0.1.255
inet6 fd80::21c:d8ff:fab7:1dba prefixlen 64 scopeid 0x20<link>
ether 00:1a:b8:d7:1a:bf txqueuelen 1000 (Ethernet)
RX packets 2295379 bytes 220126493 (209.9 MiB)
RX errors 0 dropped 31 overruns 0 frame 0
TX packets 70507 bytes 12284940 (11.7 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1458
inet 10.0.0.5 netmask 255.255.255.0 broadcast 10.0.0.255
inet6 fe81::21c:a8bf:fad7:1dca prefixlen 64 scopeid 0x20<link>
ether 00:1d:d8:b5:1c:dd txqueuelen 1000 (Ethernet)
RX packets 39090 bytes 4196802 (4.0 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 93250 bytes 18614094 (17.7 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

If one of the interfaces listed is not dedicated to only process DNS traffic, this is a finding.

Remediation:

On the host machine, configure an interface to only process DNS traffic.

Restart the host machine.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.43 BIND-9X-001530 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The platform on which the name server software is hosted must only run processes and services needed to support the BIND 9.x implementation.

```
GROUP ID: V-272406
RULE ID: SV-272406r1082266
```

Rationale:

Hosts that run the name server software should not provide any other services. Unnecessary services running on the DNS server can introduce additional attack vectors leading to the compromise of an organization's DNS architecture.

Audit:

Verify that the BIND 9.x server is dedicated for DNS traffic.

With the assistance of the DNS administrator, identify all of the processes running on the BIND 9.x server:

```
# ps -ef | less
```

If any of the identified processes are not in support of normal OS functionality or in support of the BIND 9.x process, this is a finding.

Remediation:

Disable or uninstall all non-DNS related applications from the BIND 9.x server.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.44 BIND-9X-001540 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The core BIND 9.x server files must be group owned by a group designated for DNS administration only.

```
GROUP ID: V-272407
RULE ID: SV-272407r1068060
```

Rationale:

Discretionary Access Control (DAC) is based on the premise that individual users are "owners" of objects and therefore have discretion over who should be authorized to access the object and in which mode (e.g., read or write). Ownership is usually acquired because of creating the object or via specified ownership assignment. In a DNS implementation, DAC should be granted to a minimal number of individuals and objects because DNS does not interact directly with users and users do not store and share data with the DNS application directly.

Audit:

Verify that the core BIND 9.x server files are group owned by a group designated for DNS administration only.

With the assistance of the DNS administrator, identify the following files:

```
named.conf
root hints
Primary zone file(s)
Secondary zone file(s)
```

Note: The name of the root hints file is defined in named.conf. Common names for the file are root.hints, named.cache, or db.cache.

If the identified files are not group owned by a group designated for DNS administration, this is a finding.

Remediation:

Change the ownership of the core BIND 9.x server files to the process account group.

```
# chgrp (BIND 9.x process account) <file>
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.45 BIND-9X-001550 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The core BIND 9.x server files must be owned by the root or BIND 9.x process account.

```
GROUP ID: V-272408
RULE ID: SV-272408r1068063
```

Rationale:

Discretionary Access Control (DAC) is based on the premise that individual users are "owners" of objects and therefore have discretion over who should be authorized to access the object and in which mode (e.g., read or write). Ownership is usually acquired because of creating the object or via specified ownership assignment. In a DNS implementation, DAC should be granted to a minimal number of individuals and objects because DNS does not interact directly with users and users do not store and share data with the DNS application directly.

Audit:

Verify that the core BIND 9.x server files are owned by the root or BIND 9.x process account.

With the assistance of the DNS administrator, identify the following files:

```
named.conf
root hints
Primary zone file(s)
Secondary zone files(s)
```

Note: The name of the root hints file is defined in named.conf. Common names for the file are root.hints, named.cache, or db.cache.

If the identified files are not owned by the root or BIND 9.x process account, this is a finding.

Remediation:

Change the ownership of the files to the root or BIND 9.x process account.

```
# chown <account_name> <file>
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.46 BIND-9X-001560 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The BIND 9.x server digital signature algorithm used for DNSSEC-enabled zones must be FIPS-compatible.

```
GROUP ID: V-272409
RULE ID: SV-272409r1069909
```

Rationale:

The choice of digital signature algorithm will be based on recommended algorithms in well-known standards. NIST's Digital Signature Standard (DSS) [FIPS186] provides three algorithm choices:

- Digital Signature Algorithm (DSA).
- RSA.
- Elliptic Curve DSA (ECDSA).

Of these three algorithms, RSA and DSA are more widely available and are considered candidates of choice for DNSSEC. In terms of performance, both RSA and DSA have comparable signature generation speeds, but DSA is much slower for signature verification. Hence, RSA is the recommended algorithm as far as this guideline is concerned. RSA with SHA-1 is currently the only cryptographic algorithm mandated to be implemented with DNSSEC, although other algorithm suites (i.e., RSA/SHA-256, ECDSA) are also specified. It can be expected that name servers and clients will be able to use the RSA algorithm at a minimum. It is suggested that at least one ZSK for a zone use the RSA algorithm.

NIST's Secure Hash Standard (SHS) (FIPS 180-3) specifies SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 as approved hash algorithms to be used as part of the algorithm suite for generating digital signatures using the digital signature algorithms in NIST's DSS[FIPS186]. It is expected that there will be support for Elliptic Curve Cryptography in the DNSSEC. The migration path for USG DNSSEC operation will be to ECDSA (or similar) from RSA/SHA-1 and RSA/SHA-256 before September 30th, 2015.

Audit:

Verify that the DNSSEC and TSIG keys used by the BIND 9.x implementation are FIPS 180-3 compliant.

If the server is in a classified network, the DNSSEC portion of the requirement is Not Applicable.

DNSSEC KEYS:

Inspect the "named.conf" file and identify all of the DNSSEC signed zone files:

```
zone "example.com" {
file "signed_zone_file";
};
```

For each signed zone file identified, inspect the file for the "DNSKEY" records:

```
86400 DNSKEY 257 3 8 (
<KEY HASH>
) ; KSK;
86400 DNSKEY 256 3 8 (
<KEY HASH>
) ; ZSK;
```

The fifth field in the above example identifies what algorithm was used to create the DNSKEY.

If the fifth field the KSK DNSKEY is less than "8" (SHA256), this is a finding.

If the algorithm used to create the ZSK is less than "8" (SHA256), this is a finding.

TSIG KEYS:

Inspect the "named.conf" file and identify all of the TSIG key statements:

```
key tsig_example. {
algorithm hmac-SHA256;
include "tsig-example.key";
};
```

If each key statement does not use "hmac-SHA256" or a stronger algorithm, this is a finding.

Remediation:

Create new DNSSEC and TSIG keys using a FIPS 180-3 approved cryptographic algorithm that meets or exceeds the strength of SHA256.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.47 BIND-9X-001570 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

On a BIND 9.x server all authoritative name servers for a zone must have the same version of zone information.

```
GROUP ID: V-272410
RULE ID: SV-272410r1068069
```

Rationale:

It is important to maintain the integrity of a zone file. The serial number of the SOA record is used to indicate to secondary name server that a change to the zone has occurred and a zone transfer should be performed. The serial number used in the SOA record provides the DNS administrator a method to verify the integrity of the zone file based on the serial number of the last update and ensure that all Secondary servers are using the correct zone file.

Audit:

Verify that the SOA record is at the same version for all authoritative servers for a specific zone.

With the assistance of the DNS administrator, identify each name server that is authoritative for each zone.

Inspect each zone file that the server is authoritative for and identify the following:

```
example.com. 86400 IN SOA ns1.example.com. root.example.com.
(17760704;serial)
```

If the SOA "serial" numbers are not identical on each authoritative name server, this is a finding.

Remediation:

Edit the zone file.

Update the SOA record serial number.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.48 BIND-9X-001580 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

On the BIND 9.x server CNAME records must not point to a zone with lesser security for more than six months.

```
GROUP ID: V-272411
RULE ID: SV-272411r1069910
```

Rationale:

The use of CNAME records for exercises, tests, or zone-spanning aliases should be temporary (e.g., to facilitate a migration). When a host name is an alias for a record in another zone, an adversary has two points of attack: the zone in which the alias is defined and the zone authoritative for the alias's canonical name. This configuration also reduces the speed of client resolution because it requires a second lookup after obtaining the canonical name. Furthermore, in the case of an authoritative name server, this information is promulgated throughout the enterprise to caching servers and thus compounds the vulnerability.

Audit:

Verify that the zone files used by the BIND 9.x server do not contain resource records for a domain in which the server is not authoritative.

Inspect the "named.conf" file for the following:

```
zone example.com {
file "db.example.com.signed";
};
```

Inspect each zone file for "CNAME" records and verify with the DNS administrator that these records are less than six months old.

The exceptions are glue records supporting zone delegations, CNAME records supporting a system migration, or CNAME records that point to third-party Content Delivery Networks (CDN) or cloud computing platforms. In the case of third-party CDNs or cloud offerings, an approved mission need must be demonstrated.

If there are CNAME records that point to third-party Content Delivery Networks (CDNs) or cloud computing platforms without an authorizing official (AO)-approved and documented mission need, this is a finding.

If a CNAME record is more than six months old, excluding the above, this is a finding.

Remediation:

In the case of third-party CDNs or cloud offerings, document the mission need with the AO.

Edit the zone file.

Remove CNAME records that are older than six months that do not meet the CDN or cloud offering criteria.

Restart the BIND 9.x process.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.49 BIND-9X-001590 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

On the BIND 9.x server a zone file must not include resource records that resolve to a fully qualified domain name residing in another zone.

```
GROUP ID: V-272412
RULE ID: SV-272412r1068075
```

Rationale:

If a name server were able to claim authority for a resource record in a domain for which it was not authoritative, this would pose a security risk. In this environment, an adversary could use illicit control of a name server to impact IP address resolution beyond the scope of that name server (i.e., by claiming authority for records outside of that server's zones). Fortunately, all but the oldest versions of BIND and most other DNS implementations do not allow for this behavior. Nevertheless, the best way to eliminate this risk is to eliminate from the zone files any records for hosts in another zone.

The exceptions are glue records supporting zone delegations, CNAME records supporting a system migration, or CNAME records that point to third-party Content Delivery Networks (CDN) or cloud computing platforms. In the case of third-party CDNs or cloud offerings, an approved mission need must be demonstrated.

Audit:

Verify that the zone files used by the BIND 9.x server do not contain resource records for a domain in which the server is not authoritative.

The exceptions are glue records supporting zone delegations, CNAME records supporting a system migration, or CNAME records that point to third-party Content Delivery Networks (CDN) or cloud computing platforms. In the case of third-party CDNs or cloud offerings, an approved mission need must be demonstrated.

Inspect the "named.conf" file to identify the zone files, for which the server is authoritative:

```
zone example.com {
file "db.example.com.signed";
};
```

Inspect each zone file for which the server is authoritative.

If there are CNAME records that point to third-party Content Delivery Networks (CDN) or cloud computing platforms without an authorizing official (AO)-approved and documented mission need, this is a finding.

If a zone file contains records that resolve to another zone, excluding the above, this is a finding.

Remediation:

In the case of third-party CDNs or cloud offerings, document the mission need with the AO.

Edit the zone file.

Remove any record that points to a different zone, with the exception of approved CDNs or cloud offerings.

Restart the BIND 9.x process.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.50 BIND-9X-001600 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The BIND 9.x name server software must run with restricted privileges.

```
GROUP ID: V-272413
RULE ID: SV-272413r1068078
```

Rationale:

Failure to provide logical access restrictions associated with changes to application configuration may have significant effects on the overall security of the system. When dealing with access restrictions pertaining to change control, it should be noted that any changes to the hardware, software, and/or firmware components of the information system and/or application can have significant effects on the overall security of the system. Accordingly, only qualified and authorized individuals should be allowed to obtain access to application components for the purposes of initiating changes, including upgrades and modifications.

Logical access restrictions include, for example, controls that restrict access to workflow automation, media libraries, abstract layers (e.g., changes implemented into third-party interfaces rather than directly into information systems), and change windows (e.g., changes occur only during specified times, making unauthorized changes easy to discover).

If the name server software is run as a privileged user (e.g., root in Unix systems), any break-in into the software can have disastrous consequences in terms of resources resident in the name server platform. Specifically, a hacker who breaks into the software acquires unrestricted access and therefore can execute any commands or modify or delete any files. It is necessary to run the name server software as a nonprivileged user with access restricted to specified directories to contain damages resulting from break-in.

Audit:

Verify the BIND 9.x process is not running as root:

```
# ps -ef | grep named

named 3015 1 0 12:59 ? 00:00:00 /usr/sbin/named -u named -t /var/named/chroot
```

If the output shows "/usr/sbin/named -u root", this is a finding.

Remediation:

Configure the BIND 9.x process to run as a nonprivileged user.

Restart the BIND 9.x process.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.51 BIND-9X-001610 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The BIND 9.x implementation must not use a TSIG or DNSSEC key for more than one year.

```
GROUP ID: V-272414
RULE ID: SV-272414r1082268
```

Rationale:

Configuration settings are the set of parameters that can be changed that affect the security posture and/or functionality of the system. Security-related parameters are those parameters impacting the security state of the application, including the parameters required to satisfy other security control requirements.

Configuring the DNS server implementation to follow organizationwide security implementation guides and security checklists ensures compliance with federal standards and establishes a common security baseline across DOD that reflects the most restrictive security posture consistent with operational requirements.

Audit:

With the assistance of the DNS administrator, identify all of the cryptographic key files used by the BIND 9.x implementation.

With the assistance of the DNS administrator, determine the location of the cryptographic key files used by the BIND 9.x implementation.

```
# ls -al <Crypto_Key_Location>
-rw-------. 1 named named 76 May 10 20:35 crypto-example.key
```

If the server is in a classified network, the DNSSEC portion of the requirement is Not Applicable.

For DNSSEC keys:

Verify that the "Created" date is less than one year from the date of inspection:

Note: The date format will be displayed in YYYYMMDDHHMMSS.

```
# cat <DNSSEC_Key_File> | grep -i "created"
Created: 20160704235959
```

If the "Created" date is more than one year old, this is a finding.

For TSIG keys:

Verify with the information system security officer (ISSO)/information system security manager (ISSM) that the TSIG keys are less than one year old.

If a TSIG key is more than one year old, this is a finding.

Remediation:

Generate new DNSSEC and TSIG keys.

For DNSSEC keys:

Use the newly generated keys to resign all of the zone files on the name server.

For TSIG keys:

Update the named.conf file with the new keys.

Restart the BIND 9.x process.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.52 BIND-9X-001620 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The permissions assigned to the core BIND 9.x server files must be set to use the least privilege possible.

```
GROUP ID: V-272415
RULE ID: SV-272415r1068084
```

Rationale:

Discretionary Access Control (DAC) is based on the premise that individual users are "owners" of objects and therefore have discretion over who should be authorized to access the object and in which mode (e.g., read or write). Ownership is usually acquired because of creating the object or via specified ownership assignment. In a DNS implementation, DAC should be granted to a minimal number of individuals and objects because DNS does not interact directly with users and users do not store and share data with the DNS application directly.

Audit:

With the assistance of the DNS administrator, identify the following files:

```
named.conf : rw-r-----
root hints : rw-r-----
Primary zone file(s): rw-r-----
Secondary zone file(s): rw-rw----
```

Note: The name of the root hints file is defined in named.conf. Common names for the file are root.hints, named.cache, or db.cache.

Verify that the permissions for the core BIND 9.x server files are at least as restrictive as listed above.

If the identified files are not as least as restrictive as listed above, this is a finding.

Remediation:

Configure the permissions of each file to the following:

```
named.conf : rw-r-----
root hints : rw-r-----
Primary zone file(s): rw-r-----
Secondary zone file(s): rw-rw----
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.53 BIND-9X-001630 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The host running a BIND 9.x implementation must implement a set of firewall rules that restrict traffic on the DNS interface.

```
GROUP ID: V-272416
RULE ID: SV-272416r1082270
```

Rationale:

Configuring hosts that run a BIND 9.x implementation to only accept DNS traffic on a DNS interface allows a system firewall to be configured to limit the allowed incoming ports/protocols to 53/tcp and 53/udp. Sending outgoing DNS messages from a random port minimizes the risk of an attacker guessing the outgoing message port and sending forged replies.

The TCP/IP stack in DNS hosts (stub resolver, caching/resolving/recursive name server, authoritative name server, etc.) could be subjected to packet flooding attacks (such as SYNC and smurf), resulting in disruption of communication. By implementing a specific set of firewall rules that limit accepted traffic to the interface, these risk of packet flooding and other TCP/IP based attacks is reduced.

Audit:

With the assistance of the DNS administrator, verify that the OS firewall is configured to only allow incoming messages on ports 53/tcp and 53/udp.

Note: The following rules are for the IPTables firewall. If the system is using a different firewall, the rules may be different.

Inspect the hosts firewall rules for the following rules:

```
-A INPUT -i [DNS Interface] -p tcp --dport 53 -j ACCEPT
-A INPUT -i [DNS Interface] -p udp --dport 53 -j ACCEPT
-A INPUT -i [DNS Interface] -j DROP
```

If any of the above rules do not exist, this is a finding.

If rules are listed that allow traffic on ports other than 53/tcp and 53/udp, this is a finding.

Remediation:

Configure the OS firewall to only allow incoming DNS traffic on ports 53/tcp and 53/udp.

Add the following rules to the host firewall rule set:

```
# iptables -A INPUT -i [DNS Interface] -p tcp --dport 53 -j ACCEPT
# iptables -A INPUT -i [DNS Interface] -p udp --dport 53 -j ACCEPT
# iptables -A INPUT -i [DNS Interface] -j DROP
```

Note: If the system is not using an IPTables firewall, the appropriate firewall rules that limit traffic to ports 53/tcp and 53/udp should be configured on the active firewall.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.54 BIND-9X-001650 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

A BIND 9.x server implementation must maintain the integrity and confidentiality of DNS information while it is being prepared for transmission, in transmission, and in use and must perform integrity verification and data origin verification for all DNS information.

```
GROUP ID: V-272417
RULE ID: SV-272417r1082273
```

Rationale:

DNSSEC is required for securing the DNS query/response transaction by providing data origin authentication and data integrity verification through signature verification and the chain of trust.

Failure to accomplish data origin authentication and data integrity verification could have significant effects on DNS infrastructure. The resultant response could be forged, it may have come from a poisoned cache, the packets could have been intercepted without the resolver's knowledge, or resource records could have been removed that would result in query failure or denial of service.

Failure to validate name server replies would cause many networking functions and communications to be adversely affected. With DNS, the presence of Delegation Signer (DS) records associated with child zones informs clients of the security status of child zones. These records are crucial to the DNSSEC chain of trust model. Each parent domain's DS record is used to verify the DNSKEY record in its subdomain, from the top of the DNS hierarchy down.

Failure to validate the chain of trust used with DNSSEC would have a significant impact on the security posture of the DNS server. Nonvalidated trust chains may contain rouge DNS servers and allow those unauthorized servers to introduce invalid data into an organizations DNS infrastructure. A compromise of this type would be difficult to detect and may have devastating effects on the validity and integrity of DNS zone information.

Satisfies: SRG-APP-000348-DNS-000042, SRG-APP-000420-DNS-000053, SRG-APP-000213-DNS-000024, SRG-APP-000219-DNS-000028, SRG-APP-000219-DNS-000029, SRG-APP-000219-DNS-000030, SRG-APP-000215-DNS-000026, SRG-APP-000347-DNS-000041, SRG-APP-000349-DNS-000043, SRG-APP-000441-DNS-000066, SRG-APP-000442-DNS-000067, SRG-APP-000422-DNS-000055, SRG-APP-000421-DNS-000054, SRG-APP-000423-DNS-000056, SRG-APP-000424-DNS-000057, SRG-APP-000425-DNS-000058, SRG-APP-000426-DNS-000059, SRG-APP-000251-DNS-000037

Audit:

If the server is forwarding all queries to the ERS, this is Not Applicable as the ERS validates.

Verify that DNSSEC is enabled.

Inspect the "named.conf" file for the following:

```
dnssec-enable yes;
```

If "dnssec-enable" does not exist or is not set to "yes", this is a finding.

Verify that each zone on the name server has been signed.

Identify each zone file that the name sever is responsible for and search each file for the "DNSKEY" entries:

```
# less <signed_zone_file>
86400 DNSKEY 257 3 8 ( HASHED_KEY ) ; KSK; alg = ECDSAP256SHA256; key id =
31225
86400 DNSKEY 256 3 8 ( HASHED_KEY ) ; ZSK; alg = ECDSAP256SHA256; key id =
52179
```

Ensure that there are separate "DNSKEY" entries for the "KSK" and the "ZSK".

If the "DNSKEY" entries are missing, the zone file is not signed.

If the zone files are not signed, this is a finding.

Remediation:

Set the "dnssec-enable" option to "yes".

Sign each zone file for which the name server is responsible.

Configure each zone the name server is responsible for to use a DNSSEC signed zone.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

CCI-001902 Provide the means for authorized individuals to determine the identity of the producer of the information.

- NIST SP 800-53 Revision 4::AU-10 (1) (b)
- NIST SP 800-53 Revision 5::AU-10 (1) (b)

CCI-002463 Provide data origin artifacts for internal name/address resolution queries.

- NIST SP 800-53 Revision 4::SC-20 (2)
- NIST SP 800-53 Revision 5::SC-20 (2)

CCI-001178 Provide additional data origin authentication artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries.

- NIST SP 800-53::SC-20
- NIST SP 800-53A::SC-20.1
- NIST SP 800-53 Revision 4::SC-20 a
- NIST SP 800-53 Revision 5::SC-20 a

CCI-001184 Protect the authenticity of communications sessions.

- NIST SP 800-53::SC-23
- NIST SP 800-53A::SC-23.1
- NIST SP 800-53 Revision 4::SC-23
- NIST SP 800-53 Revision 5::SC-23

CCI-001663 The information system, when operating as part of a distributed, hierarchical namespace, provides the means to enable verification of a chain of trust among parent and child domains (if the child supports secure resolution services).

- NIST SP 800-53::SC-20 (1)
- NIST SP 800-53A::SC-20 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-20 b
- NIST SP 800-53 Revision 5::SC-20 b

CCI-001901 Bind the identity of the information producer with the information to an organization-defined strength of binding.

- NIST SP 800-53 Revision 4::AU-10 (1) (a)
- NIST SP 800-53 Revision 5::AU-10 (1) (a)

CCI-001904 Validate the binding of the information producer identity to the information at an organization-defined frequency.

- NIST SP 800-53 Revision 4::AU-10 (2) (a)
- NIST SP 800-53 Revision 5::AU-10 (2) (a)

CCI-002420 Maintain the confidentiality and/or integrity of information during preparation for transmission.

- NIST SP 800-53 Revision 4::SC-8 (2)
- NIST SP 800-53 Revision 5::SC-8 (2)

CCI-002422 Maintain the confidentiality and/or integrity of information during reception.

- NIST SP 800-53 Revision 4::SC-8 (2)
- NIST SP 800-53 Revision 5::SC-8 (2)

CCI-002462 Provide additional data integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries.

- NIST SP 800-53 Revision 4::SC-20 a
- NIST SP 800-53 Revision 5::SC-20 a

CCI-002464 Provide data integrity protection artifacts for internal name/address resolution queries.

- NIST SP 800-53 Revision 4::SC-20 (2)
- NIST SP 800-53 Revision 5::SC-20 (2)

CCI-002465 Request data origin authentication verification on the name/address resolution responses the system receives from authoritative sources.

- NIST SP 800-53 Revision 4::SC-21
- NIST SP 800-53 Revision 5::SC-21

CCI-002466 Request data integrity verification on the name/address resolution responses the system receives from authoritative sources.

- NIST SP 800-53 Revision 4::SC-21
- NIST SP 800-53 Revision 5::SC-21

CCI-002467 Perform data integrity verification on the name/address resolution responses the system receives from authoritative sources.

- NIST SP 800-53 Revision 4::SC-21
- NIST SP 800-53 Revision 5::SC-21

CCI-002468 Perform data origin verification authentication on the name/address resolution responses the system receives from authoritative sources.

- NIST SP 800-53 Revision 4::SC-21
- NIST SP 800-53 Revision 5::SC-21

CCI-001310 Checks the validity of organization-defined information inputs to the system.

- NIST SP 800-53::SI-10
- NIST SP 800-53A::SI-10.1
- NIST SP 800-53 Revision 4::SI-10
- NIST SP 800-53 Revision 5::SI-10

1.55 BIND-9X-001660 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

In the event of an error when validating the binding of other DNS servers' identity to the BIND 9.x information, when anomalies in the operation of the signed zone transfers are discovered, for the success and failure of start and stop of the name server service or daemon, and for the success and failure of all name server events, a BIND 9.x server implementation must generate a log entry.

```
GROUP ID: V-272418
RULE ID: SV-272418r1068281
```

Rationale:

Auditing and logging are key components of any security architecture. It is essential for security personnel to know what is being performed on the system, where an event occurred, when an event occurred, and by whom the event was triggered, to compile an accurate risk assessment. Logging the actions of specific events provides a means to investigate an attack, to recognize resource utilization or capacity thresholds, or to simply identify an improperly configured DNS system. If auditing is not comprehensive, it will not be useful for intrusion monitoring, security investigations, and forensic analysis.

The DNS server should audit all failed attempts at server authentication through DNSSEC and TSIG. The actual auditing is performed by the OS/NDM but the configuration to trigger the auditing is controlled by the DNS server.

Failing to act on the validation errors may result in the use of invalid, corrupted, or compromised information. The validation of bindings can be achieved, for example, by the use of cryptographic checksums. Validations must be performed automatically.

The DNS server does not have the capability of shutting down or restarting the information system. The DNS server can be configured to generate audit records when anomalies are discovered.

Satisfies: SRG-APP-000350-DNS-000044, SRG-APP-000089-DNS-000005, SRG-APP-000504-DNS-000074, SRG-APP-000504-DNS-000082, SRG-APP-000474-DNS-000073

Audit:

Verify the name server is configured to log error messages with a severity of "info":

Inspect the "named.conf" file for the following:

```
logging {
channel channel_name {
severity info;
};
```

If the "severity" sub statement is not set to "info", this is a finding.

Note: Setting the "severity" sub statement to "info" will log all messages for the following severity levels: Critical, Error, Warning, Notice, and Info.

Remediation:

Edit the "named.conf" file.

Add the "severity" sub statement to the "channel" statement.

Configure the "severity" sub statement to "info".

Restart the BIND 9.x process.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

CCI-001906 Perform organization-defined actions in the event of an error when validating the binding of the information producer identity to the information.

- NIST SP 800-53 Revision 4::AU-10 (2) (b)
- NIST SP 800-53 Revision 5::AU-10 (2) (b)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a
- NIST SP 800-53 Revision 5::AU-12 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-002702 Shut the system down, restart the system, and/or initiate organization-defined alternative action(s) when anomalies in the operation of the organization-defined security functions are discovered.

- NIST SP 800-53 Revision 4::SI-6 d
- NIST SP 800-53 Revision 5::SI-6 d

1.56 BIND-9X-001680 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The BIND 9.x server implementation must be configured to use only approved ports and protocols.

```
GROUP ID: V-272419
RULE ID: SV-272419r1068096
```

Rationale:

To prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling (i.e., embedding of data types within data types), organizations must disable or restrict unused or unnecessary physical and logical ports/protocols on information systems.

Applications are capable of providing a wide variety of functions and services. Some of the functions and services provided by default may not be necessary to support essential organizational operations. Additionally, it is sometimes convenient to provide multiple services from a single component (e.g., email and web services); however, doing so increases risk over limiting the services provided by any one component.

To support the requirements and principles of least functionality, the application must support the organizational requirements by providing only essential capabilities and limiting the use of ports, protocols, and/or services to only those required, authorized, and approved to conduct official business or to address authorized quality of life issues.

Audit:

Verify the BIND 9.x server is configured to listen on UDP/TCP port 53.

Inspect the "named.conf" file for the following:

```
options {
listen-on port 53 { <ip_address>; };
};
```

If the "port" variable is missing, this is a finding.

If the "port" variable is not set to "53", this is a finding.

Note: "<ip_address>" should be replaced with the DNS server IP address.

Remediation:

Edit the "named.conf" file.

Add the following line to the "options" statement:

```
listen-on port 53 { <ip_address>; };
```

Replace "<ip_address>" with the IP of the name server.

Restart the BIND 9.x process.

Additional Information:

CCI-000382 Configure the system to prohibit or restrict the use of organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (iii)
- NIST SP 800-53 Revision 4::CM-7 b
- NIST SP 800-53 Revision 5::CM-7 b

1.57 BIND-9X-001690 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The BIND 9.x server implementation must uniquely identify and authenticate the other DNS server before responding to a server-to-server transaction, zone transfer and/or dynamic update request using cryptographically based bidirectional authentication to protect the integrity of the information in transit.

```
GROUP ID: V-272420
RULE ID: SV-272420r1082275
```

Rationale:

Server-to-server (zone transfer) transactions are provided by TSIG, which enforces mutual server authentication using a key that is unique to each server pair (TSIG), thus uniquely identifying the other server.

Enforcing separate TSIG key-pairs provides another layer of protection for the BIND implementation in the event that a TSIG key is compromised. This additional layer of security provides the DNS administrators with the ability to change a compromised TSIG key with a minimal disruption to DNS operations.

Failure to identify devices and authenticate devices can lead to malicious activity, such as a Man-In-The-Middle attack where an attacker could pose as an authorized name server and redirect legitimate customers to malicious websites. A failure on this part could also lead to a Denial of Service of any and all DNS services provided to an organizations network infrastructure.

Audit:

If zone transfers are disabled with the "allow-transfer { none; };" directive, this is Not Applicable.

Verify that the BIND 9.x server is configured to uniquely identify a name server before responding to a zone transfer.

Inspect the "named.conf" file for the presence of TSIG key statements.

On the primary name server, this is an example of a configured key statement:

```
key tsig_example. {
algorithm hmac-SHA1;
include "tsig-example.key";
};

zone "disa.mil" {
type Primary;
file "db.disa.mil";
allow-transfer { key tsig_example.; };
};
```

On the secondary name server, this is an example of a configured key statement:

```
key tsig_example. {
algorithm hmac-SHA1;
include "tsig-example.key";
};

server <ip_address> {
keys { tsig_example };
};

zone "disa.mil" {
type Secondary;
Primarys { <ip_address>; };
file "db.disa.mil";
};
```

If a primary name server does not have a key defined in the "allow-transfer" block, this is a finding.

If a secondary name server does not have a server statement that contains a "keys" sub statement, this is a finding.

Remediation:

Configure the BIND 9.x server to use TSIG keys.

Add a key statement to the "named.conf" file for TSIG that is being used:

```
key tsig_example. {
algorithm hmac-SHA1;
include "tsig-example.key";
};
```

Add key statements to the allow-transfer statements on a primary name server:

```
allow-transfer { key tsig_example.; };
```

Add key statements to the server statements on a secondary name server:

```
server <ip_address> {
keys { tsig_example };
};
```

Restart the BIND 9.x process.

Additional Information:

CCI-000778 Uniquely identify organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection.

- NIST SP 800-53::IA-3
- NIST SP 800-53A::IA-3.1 (ii)
- NIST SP 800-53 Revision 4::IA-3
- NIST SP 800-53 Revision 5::IA-3

1.58 BIND-9X-001700 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The BIND 9.x server implementation must use separate TSIG key-pairs when securing server-to-server transactions.

```
GROUP ID: V-272421
RULE ID: SV-272421r1068102
```

Rationale:

Without identifying devices, unidentified or unknown devices may be introduced, thereby facilitating malicious activity. This applies to server-to-server (zone transfer) transactions only and is provided by TSIG/SIG(0), which enforces mutual server authentication using a key that is unique to each server pair (TSIG) or using PKI-based authentication (SIG[0]), thus uniquely identifying the other server.

Audit:

Verify that the BIND 9.x server is configured to use separate TSIG key-pairs when securing server-to-server transactions.

Inspect the "named.conf" file for the presence of TSIG key statements:

On the primary name server, this is an example of a configured key statement:

```
key tsig_example. {
algorithm hmac-SHA1;
include "tsig-example.key";
};

zone "disa.mil" {
type Primary;
file "db.disa.mil";
allow-transfer { key tsig_example.; };
};
```

On the secondary name server, this is an example of a configured key statement:

```
key tsig_example. {
algorithm hmac-SHA1;
include "tsig-example.key";
};

server <ip_address> {
keys { tsig_example };
};

zone "disa.mil" {
type Secondary;
Primarys { <ip_address>; };
file "db.disa.mil";
};
```

Verify that each TSIG key-pair listed is only used by a single key statement:

```
# cat <tsig_key_file>
```

If any TSIG key-pair is being used by more than one key statement, this is a finding.

Remediation:

Create a separate TSIG key-pair for each key statement listed in the named.conf file.

Configure the name server to use separate TSIG key-pairs for each key statement listed in the named.conf file.

Restart the BIND 9.x process.

Additional Information:

CCI-000778 Uniquely identify organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection.

- NIST SP 800-53::IA-3
- NIST SP 800-53A::IA-3.1 (ii)
- NIST SP 800-53 Revision 4::IA-3
- NIST SP 800-53 Revision 5::IA-3

1.59 BIND-9X-001720 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

A BIND 9.x server implementation must be running in a chroot(ed) directory structure.

```
GROUP ID: V-272422
RULE ID: SV-272422r1068105
```

Rationale:

With any network service, there is the potential that an attacker can exploit a vulnerability within the program that allows the attacker to gain control of the process and even run system commands with that control. One possible defense against this attack is to limit the software to particular quarantined areas of the file system, memory or both. This effectively restricts the service so that it will not have access to the full file system. If such a defense were in place, then even if an attacker gained control of the process, the attacker would be unable to reach other commands or files on the system. This approach often is referred to as a padded cell, jail, or sandbox. All of these terms allude to the fact that the software is contained in an area where it cannot harm either itself or others. A more technical term is a chroot(ed) directory structure.

BIND should be configured to run in a padded cell or chroot(ed) directory structure.

Audit:

Verify the directory structure where the primary BIND 9.x server configuration files are stored is running in a chroot(ed) environment or a containerized environment:

```
# ps -ef | grep named

named 3015 1 0 12:59 ? 00:00:00 /usr/sbin/named -u named -t /var/named/chroot
```

If the output does not contain "-t <chroot_path>", this is a finding.

Remediation:

Configure the BIND 9.x server to operate in a chroot(ed) directory structure.

Additional Information:

CCI-001090 Prevent unauthorized and unintended information transfer via shared system resources.

- NIST SP 800-53::SC-4
- NIST SP 800-53A::SC-4.1
- NIST SP 800-53 Revision 4::SC-4
- NIST SP 800-53 Revision 5::SC-4

1.60 BIND-9X-001740 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

A BIND 9.x implementation configured as a caching name server must restrict recursive queries to only the IP addresses and IP address ranges of known supported clients.

```
GROUP ID: V-272423
RULE ID: SV-272423r1068108
```

Rationale:

Any host that can query a resolving name server has the potential to poison the servers name cache or take advantage of other vulnerabilities that may be accessed through the query service. The best way to prevent this type of attack is to limit queries to internal hosts, which need to have this service available to them.

To guard against poisoning, name servers authoritative for .mil domains should be separated functionally from name servers that resolve queries on behalf of internal clients. Organizations may achieve this separation by dedicating machines to each function or, if possible, by running two instances of the name server software on the same machine: one for the authoritative function and the other for the resolving function. In this design, each name server process may be bound to a different IP address or network interface to implement the required segregation.

Audit:

This check is only applicable to caching name servers.

Verify the allow-query and allow-recursion phrases are properly configured.

Inspect the "named.conf" file for the following:

```
allow-query {trustworthy_hosts;};
allow-recursion {trustworthy_hosts;};
```

The name of the ACL does not need to be "trustworthy_hosts" but the name should match the ACL name defined earlier in "named.conf" for this purpose. If not, this is a finding.

Verify noninternal IP addresses do not appear in either the referenced ACL (e.g., trustworthy_hosts) or directly in the statements themselves.

If noninternal IP addresses appear, this is a finding.

Remediation:

Configure the caching name server to accept recursive queries only from the IP addresses and address ranges of known supported clients.

Edit the "named.conf" file and add the following to the options statement:

```
allow-query {trustworthy_hosts;};
allow-recursion {trustworthy_hosts;};
```

Restart the BIND 9.x process.

Additional Information:

CCI-001094 Restrict the ability of individuals to launch organization-defined denial of service attacks against other systems.

- NIST SP 800-53::SC-5 (1)
- NIST SP 800-53A::SC-5 (1).1
- NIST SP 800-53 Revision 4::SC-5 (1)
- NIST SP 800-53 Revision 5::SC-5 (1)

1.61 BIND-9X-001750 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

A BIND 9.x server implementation must manage excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service (DoS) attacks.

```
GROUP ID: V-272424
RULE ID: SV-272424r1069912
```

Rationale:

A DoS is a condition when a resource is not available for legitimate users. When this occurs, the organization either cannot accomplish its mission or must operate at degraded capacity.

A DoS attack against the DNS infrastructure has the potential to cause a DoS to all network users. As the DNS is a distributed backbone service of the Internet, various forms of amplification attacks resulting in DoS, while using the DNS, are still prevalent on the internet today. Some potential DoS flooding attacks against the DNS include malformed packet flood, spoofed source addresses, and distributed DoS. Without the DNS, users and systems would not have the ability to perform simple name to IP resolution.

Configuring the DNS implementation to defend against cache poisoning, employing increased capacity and bandwidth, building redundancy into the DNS architecture, using DNSSEC, limiting and securing recursive services, DNS black holes, etc., may reduce the susceptibility to some flooding types of DoS attacks.

Audit:

If this is a recursive name server, this is Not Applicable.

Note: A recursive name server should NOT be configured as an authoritative name server for any zone.

Verify that the BIND 9.x server is configured to prohibit recursion on authoritative name servers.

Inspect the "named.conf" file for the following:

```
options {
recursion no;
allow-query {none;};
};
```

If the "recursion" sub statement is missing, or set to "yes", this is a finding.

If the "allow-query" sub statement under the "options statement" is not set to "none", this is a finding.

Verify that an "allow-query" sub statement under each zone statement is configured to authorized hosts:

```
zone "example.com" {
type Primary;
file "db.example.com";
allow-query { (address_match_list | <ip_address>) };
};
```

If the "allow-query" sub statement under each zone statement is not restricted to authorized hosts, this is a finding.

Remediation:

Configure the authoritative name server to prohibit recursion.

Edit the "named.conf" file and add the following sub statements to the options statement:

```
recursion no;
allow-query { none };
```

Configure each zone to limit queries to authorized hosts:

Edit the "named.conf" file and add the following sub statement to each zone definition:

```
allow-query { address_match_list; };
```

Restart the BIND 9.x process.

Additional Information:

CCI-001095 Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service attacks.

- NIST SP 800-53::SC-5 (2)
- NIST SP 800-53A::SC-5 (2).1
- NIST SP 800-53 Revision 4::SC-5 (2)
- NIST SP 800-53 Revision 5::SC-5 (2)

1.62 BIND-9X-001770 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

A BIND 9.x server implementation must provide the means to indicate the security status of child zones.

```
GROUP ID: V-272425
RULE ID: SV-272425r1068114
```

Rationale:

If name server replies are invalid or cannot be validated, many networking functions and communication would be adversely affected. With DNS, the presence of Delegation Signer (DS) records associated with child zones informs clients of the security status of child zones. These records are crucial to the DNSSEC chain of trust model. Each parent domain's DS record is used to verify the DNSKEY record in its subdomain, from the top of the DNS hierarchy down.

A DNS server is an example of an information system providing name/address resolution service. Digital signatures and cryptographic keys are examples of additional artifacts. DNS resource records are examples of authoritative data. Applications other than the DNS, to map between host/service names and network addresses, must provide other means to ensure the authenticity and integrity of response data.

In DNS, trust in the public key of the source is established by starting from a trusted name server and establishing the chain of trust down to the current source of response through successive verifications of signature of the public key of a child by its parent.

A trust anchor is an authoritative entity represented via a public key and associated data. It is used in the context of public key infrastructures, X.509 digital certificates, and DNSSEC.

When there is a chain of trust, usually the top entity to be trusted becomes the trust anchor. A certification path starts with the subject certificate and proceeds through a number of intermediate certificates up to a trusted root certificate. In DNS, a trust anchor is a DNSKEY that is placed into a validating resolver so the validator can cryptographically validate the results for a given request back to a known public key (the trust anchor).

An example means to indicate the security status of child subspaces is using delegation signer (DS) resource records in the DNS.

Path validation is necessary for a relying party to make an informed trust decision when presented with any certificate not already explicitly trusted. Without path validation and a chain of trust, there can be no trust that the data integrity authenticity has been maintained during a transaction.

Audit:

Verify that there is a DS record set for each child zone defined in "/etc/named.conf" file.

For each child zone listed in "/etc/named.conf" file, verify there is a corresponding "dsset-zone_name" file.

If any child zone does not have a corresponding DS record set, this is a finding.

Remediation:

Sign each child zone. During the zone signing process, ensure that a DS record is created and is stored on the parent zone name server.

Additional Information:

CCI-001179 Provides the means to indicate the security status of child zones, when operating as part of a distributed, hierarchical namespace.

- NIST SP 800-53::SC-20 (1)
- NIST SP 800-53A::SC-20 (1).1 (i)
- NIST SP 800-53 Revision 4::SC-20 b
- NIST SP 800-53 Revision 5::SC-20 b

1.63 BIND-9X-001780 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The BIND 9.x server validity period for the RRSIGs covering the DS RR for zones delegated children must be no less than two days and no more than one week.

```
GROUP ID: V-272426
RULE ID: SV-272426r1068117
```

Rationale:

The best way for a zone administrator to minimize the impact of a key compromise is by limiting the validity period of RRSIGs in the zone and in the parent zone. This strategy limits the time during which an attacker can take advantage of a compromised key to forge responses. An attacker that has compromised a zone-signing key (ZSK) can use that key only during the key signing key's (KSK's) signature validity interval. An attacker that has compromised a KSK can use that key for only as long as the signature interval of the RRSIG covering the DS RR in the delegating parent. These validity periods should be short, which will require frequent re-signing.

To prevent the impact of a compromised KSK, a delegating parent should set the signature validity period for RRSIGs covering DS RRs in the range of a few days to 1 week. This re-signing does not require frequent rollover of the parent's ZSK, but scheduled ZSK rollover should still be performed at regular intervals.

Audit:

Note: This requirement does not validate the sig-validity-interval. This requirement ensures the signature validity period (i.e., the time from the signature's inception until the signature's expiration). It is recommended to ensure the Start of Authority (SOA) expire period (how long a secondary will still treat its copy of the zone data as valid if it cannot contact the primary.) is configured to ensure the SOA does not expire during the period of signature inception and signature expiration.

With the assistance of the DNS administrator, identify the RRSIGs that cover the DS resource records for each child zone.

Each record will list an expiration and inception date, the difference of which will provide the validity period.

The dates are listed in the following format:

```
YYYYMMDDHHMMSS
```

For each RRSIG identified, verify that the validity period is no less than two days and is no longer than seven days.

If the validity period is outside of the specified range, this is a finding.

Remediation:

Resign the child zone files and have the zone administrator provide updated DS resource records for the child zone.

Additional Information:

CCI-001179 Provides the means to indicate the security status of child zones, when operating as part of a distributed, hierarchical namespace.

- NIST SP 800-53::SC-20 (1)
- NIST SP 800-53A::SC-20 (1).1 (i)
- NIST SP 800-53 Revision 4::SC-20 b
- NIST SP 800-53 Revision 5::SC-20 b

1.64 BIND-9X-001830 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Permissions assigned to the DNSSEC keys used with the BIND 9.x implementation must enforce read-only access to the key owner and deny access to all other users.

```
GROUP ID: V-272427
RULE ID: SV-272427r1082277
```

Rationale:

Information at rest refers to the state of information when it is located on a secondary storage device within an organizational information system. Mobile devices, laptops, desktops, and storage devices can be either lost or stolen, and the contents of their data storage (e.g., hard drives and nonvolatile memory) can be read, copied, or altered. Applications and application users generate information throughout the course of their application use.

The DNS server must protect the confidentiality and integrity of the DNSSEC keys and must protect the integrity of DNS information. There is no need to protect the confidentiality of DNS information because it is accessible by all devices that can contact the server.

Audit:

Verify permissions assigned to the DNSSEC keys enforce read-only access to the key owner and deny access to group or system users.

With the assistance of the DNS administrator, determine the location of the DNSSEC keys used by the BIND 9.x implementation:

```
# ls -al <DNSSEC_Key_Location>
-r--------. 1 named named 76 May 10 20:35 DNSSEC-example.key
```

If the key files are more permissive than 400, this is a finding.

Remediation:

Change the permissions of the DNSSEC key files:

```
# chmod 400 <DNSSEC_key_file>
```

Additional Information:

CCI-001199 Protects the confidentiality and/or integrity of organization-defined information at rest.

- NIST SP 800-53::SC-28
- NIST SP 800-53A::SC-28.1
- NIST SP 800-53 Revision 4::SC-28
- NIST SP 800-53 Revision 5::SC-28

1.65 BIND-9X-001840 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The DNSSEC keys used with the BIND 9.x implementation must be owned by a privileged account.

```
GROUP ID: V-272428
RULE ID: SV-272428r1069913
```

Rationale:

Information at rest refers to the state of information when it is located on a secondary storage device within an organizational information system. Mobile devices, laptops, desktops, and storage devices can be either lost or stolen, and the contents of their data storage (e.g., hard drives and nonvolatile memory) can be read, copied, or altered. Applications and application users generate information throughout the course of their application use.

The DNS server must protect the confidentiality and integrity of the DNSSEC keys and must protect the integrity of DNS information. There is no need to protect the confidentiality of DNS information because it is accessible by all devices that can contact the server.

Audit:

With the assistance of the DNS administrator, identify all of the DNSSEC keys used by the BIND 9.x implementation.

Identify the account that the "named" process is running as:

```
# ps -ef | grep named
named 3015 1 0 12:59 ? 00:00:00 /usr/sbin/named -u named -t /var/named/chroot
```

With the assistance of the DNS administrator, determine the location of the DNSSEC keys used by the BIND 9.x implementation.

```
# ls -al <DNSSEC_Key_Location>
-r--------. 1 named named 76 May 10 20:35 DNSSEC-example.key
```

If any of the DNSSEC keys are not owned by the above account, this is a finding.

Remediation:

Change the ownership of the DNSSEC keys to the named process it is running as.

```
# chown <named_proccess_owner> <DNSSEC_key_file>.
```

Additional Information:

CCI-001199 Protects the confidentiality and/or integrity of organization-defined information at rest.

- NIST SP 800-53::SC-28
- NIST SP 800-53A::SC-28.1
- NIST SP 800-53 Revision 4::SC-28
- NIST SP 800-53 Revision 5::SC-28

1.66 BIND-9X-001850 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The DNSSEC keys used with the BIND 9.x implementation must be group owned by a privileged account.

```
GROUP ID: V-272429
RULE ID: SV-272429r1069914
```

Rationale:

Information at rest refers to the state of information when it is located on a secondary storage device within an organizational information system. Mobile devices, laptops, desktops, and storage devices can be either lost or stolen, and the contents of their data storage (e.g., hard drives and nonvolatile memory) can be read, copied, or altered. Applications and application users generate information throughout the course of their application use.

The DNS server must protect the confidentiality and integrity of the DNSSEC keys and must protect the integrity of DNS information. There is no need to protect the confidentiality of DNS information because it is accessible by all devices that can contact the server.

Audit:

With the assistance of the DNS administrator, identify all of the DNSSEC keys used by the BIND 9.x implementation.

Identify the account that the "named" process is running as:

```
# ps -ef | grep named
named 3015 1 0 12:59 ? 00:00:00 /usr/sbin/named -u named -t /var/named/chroot
```

With the assistance of the DNS administrator, determine the location of the DNSSEC keys used by the BIND 9.x implementation.

```
# ls -al <DNSSEC_Key_Location>
-r---------. 1 named named 76 May 10 20:35 DNSSEC-example.key
```

If any of the DNSSEC keys are not group owned by the above account, this is a finding.

Remediation:

Change the group ownership of the DNSSEC keys to the named process it is running as.

```
# chgrp <named_proccess_group> <DNSSEC_key_file>.
```

Additional Information:

CCI-001199 Protects the confidentiality and/or integrity of organization-defined information at rest.

- NIST SP 800-53::SC-28
- NIST SP 800-53A::SC-28.1
- NIST SP 800-53 Revision 4::SC-28
- NIST SP 800-53 Revision 5::SC-28

1.67 BIND-9X-001890 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The BIND 9.x server implementation must maintain at least three file versions of the local log file.

```
GROUP ID: V-272430
RULE ID: SV-272430r1068129
```

Rationale:

DNS software administrators require DNS transaction logs for a wide variety of reasons including troubleshooting, intrusion detection, and forensics. Ensuring that the DNS transaction logs are recorded on the local system will provide the capability needed to support these actions.

Audit:

Verify that the BIND 9.x server is configured to retain at least 3 versions of the local log file.

Inspect the "named.conf" file for the following:

```
logging {
channel local_file_channel {
file "path_name" versions 3;
};
```

If the "versions" variable is not defined, this is a finding.

If the "versions" variable is configured to retain less than three versions of the local log file, this is a finding.

Remediation:

Edit the "named.conf" file.

Add the "versions" variable to the end of the "file" sub statement in the channel statement.

Configure the "versions" sub statement to a number that is greater or equal to "3".

Restart the BIND 9.x process.

Additional Information:

CCI-001348 Store audit records on an organization-defined frequency in a repository that is part of a physically different system or system component than the system or component being audited.

- NIST SP 800-53::AU-9 (2)
- NIST SP 800-53A::AU-9 (2).1 (iii)
- NIST SP 800-53 Revision 4::AU-9 (2)
- NIST SP 800-53 Revision 5::AU-9 (2)

1.68 BIND-9X-001900 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The BIND 9.x server implementation must be configured with a channel to send audit records to a local file.

```
GROUP ID: V-272431
RULE ID: SV-272431r1068132
```

Rationale:

DNS software administrators require DNS transaction logs for a wide variety of reasons including troubleshooting, intrusion detection, and forensics. Ensuring that the DNS transaction logs are recorded on the local system will provide the capability needed to support these actions.

Audit:

Verify that the BIND 9.x server is configured to send audit logs to a local log file.

Note: syslog and local file channel must be defined for every defined category.

Inspect the "named.conf" file for the following:

```
logging {
channel local_file_channel {
file "path_name" versions 3;
print-time yes;
print-severity yes;
print-category yes;
};

category category_name { local_file_channel; };
```

If a logging channel is not defined for a local file, this is a finding.

If a category is not defined to send messages to the local file channel, this is a finding.

Remediation:

Edit the "named.conf" file and add the following:

```
logging {
channel local_file_channel {
file "path_name" versions 3;
print-time yes;
print-severity yes;
print-category yes;
};
category category_name { local_file_channel; };
};
```

Restart the BIND 9.x process.

Additional Information:

CCI-001348 Store audit records on an organization-defined frequency in a repository that is part of a physically different system or system component than the system or component being audited.

- NIST SP 800-53::AU-9 (2)
- NIST SP 800-53A::AU-9 (2).1 (iii)
- NIST SP 800-53 Revision 4::AU-9 (2)
- NIST SP 800-53 Revision 5::AU-9 (2)

1.69 BIND-9X-001910 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The BIND 9.x server implementation must be configured with a channel to send audit records to a remote syslog.

```
GROUP ID: V-272432
RULE ID: SV-272432r1082279
```

Rationale:

Protection of log data includes assuring log data is not accidentally lost or deleted. Backing up audit records to a different system or onto separate media than the system being audited on a defined frequency helps to ensure, in the event of a catastrophic system failure, the audit records will be retained.

This helps to ensure a compromise of the information system being audited does not also result in a compromise of the audit records.

Audit:

Verify that the BIND 9.x server is configured to send audit logs to the syslog service.

Note: syslog and local file channel must be defined for every defined category.

Inspect the "named.conf" file for the following:

```
logging {
channel <syslog_channel> {
syslog <syslog_facility>;
};

category <category_name> { <syslog_channel>; };
```

If a logging channel is not defined for syslog, this is a finding.

If a category is not defined to send messages to the syslog channel, this is a finding.

Ensure audit records are forwarded to a remote server:

```
# grep "\*.\*" /etc/syslog.conf |grep "@" | grep -v "^#" (for syslog)
or:
# grep "\*.\*" /etc/rsyslog.conf | grep "@" | grep -v "^#" (for rsyslog)
```

If neither of these lines exist, this is a finding.

Remediation:

Configure the "logging" statement to send audit logs to the syslog daemon.

```
logging {
channel <syslog_channel> {
syslog <syslog_facility>;
};
category <category_name> { <syslog_channel>; };
};
```

Note: It is recommended to use a local syslog facility (i.e., local0 -7) when configuring the syslog channel.

Restart the BIND 9.x process.

Configure the (r)syslog daemon to send audit logs to a remote server.

Additional Information:

CCI-001348 Store audit records on an organization-defined frequency in a repository that is part of a physically different system or system component than the system or component being audited.

- NIST SP 800-53::AU-9 (2)
- NIST SP 800-53A::AU-9 (2).1 (iii)
- NIST SP 800-53 Revision 4::AU-9 (2)
- NIST SP 800-53 Revision 5::AU-9 (2)

1.70 BIND-9X-001920 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The BIND 9.x server implementation must not be configured with a channel to send audit records to null.

```
GROUP ID: V-272433
RULE ID: SV-272433r1068138
```

Rationale:

DNS software administrators require DNS transaction logs for a wide variety of reasons including troubleshooting, intrusion detection, and forensics. Ensuring that the DNS transaction logs are recorded on the local system will provide the capability needed to support these actions. Sending DNS transaction data to the null channel would cause a loss of important data.

Audit:

Verify that the BIND 9.x server is not configured to send audit logs to the null channel.

Inspect the "named.conf" file for the following:

```
category null { null; }
```

If there is a category defined to send audit logs to the "null" channel, this is a finding.

Remediation:

Edit the "named.conf" file.

Remove any instance of the following:

```
category null { null; };
```

Restart the BIND 9.x process.

Additional Information:

CCI-001348 Store audit records on an organization-defined frequency in a repository that is part of a physically different system or system component than the system or component being audited.

- NIST SP 800-53::AU-9 (2)
- NIST SP 800-53A::AU-9 (2).1 (iii)
- NIST SP 800-53 Revision 4::AU-9 (2)
- NIST SP 800-53 Revision 5::AU-9 (2)

1.71 BIND-9X-001950 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

A BIND 9.x server implementation must enforce approved authorizations for controlling the flow of information between authoritative name servers and specified secondary name servers based on DNSSEC policies.

```
GROUP ID: V-272434
RULE ID: SV-272434r1068141
```

Rationale:

A mechanism to detect and prevent unauthorized communication flow must be configured or provided as part of the system design. If information flow is not enforced based on approved authorizations, the system may become compromised. Information flow control regulates where information is allowed to travel within a system and between interconnected systems. The flow of all application information must be monitored and controlled so it does not introduce any unacceptable risk to the systems or data.

Within the context of DNS, this is applicable in terms of controlling the flow of DNS information between systems, such as DNS zone transfers.

Authoritative name servers (especially primary name servers) should be configured with an allow-transfer access control sub statement designating the list of hosts from which DNS information, such as zone transfers, can be accepted. These restrictions address the denial-of-service (DoS) threat and potential exploits from unrestricted dissemination of information about internal resources.

Zone transfer from primary name servers should be restricted to secondary name servers. The zone transfer should be completely disabled in the secondary name servers. The address match list argument for the allow-transfer sub statement should consist of IP addresses of secondary name servers and stealth secondary name servers.

Audit:

On an authoritative name sever, verify that each zone statement defined in the "named.conf" file contains an "allow-transfer" statement.

Inspect the "named.conf" file for the following:

```
zone example.com {
allow-transfer { <ip_address_list>; };
};
```

If there is not an "allow-transfer" statement for each zone defined, or the list contains IP addresses that are not authorized for that zone, this is a finding.

On a secondary name server, verify that each zone statement defined in the "named.conf" file contains an "allow-transfer" statement.

Inspect the "named.conf" file for the following:

```
zone example.com {
allow-transfer { none; };
};
```

If there is not an "allow-transfer" statement, or the statement is not set to "none", this is a finding.

Remediation:

For an authoritative name server, configure each zone statement to allow transfers from authorized hosts:

```
allow-transfer { <ip_address_list>; };
```

Restart the BIND 9.x process.

For a secondary server, configure each zone to deny zone transfer requests:

```
allow-transfer { none; };
```

Restart the BIND 9.x process.

Additional Information:

CCI-001663 The information system, when operating as part of a distributed, hierarchical namespace, provides the means to enable verification of a chain of trust among parent and child domains (if the child supports secure resolution services).

- NIST SP 800-53::SC-20 (1)
- NIST SP 800-53A::SC-20 (1).1 (ii)
- NIST SP 800-53 Revision 4::SC-20 b
- NIST SP 800-53 Revision 5::SC-20 b

1.72 BIND-9X-002010 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The BIND 9.x server implementation must uniquely identify and authenticate the other DNS server before responding to a server-to-server transaction, zone transfer, and/or dynamic update request using cryptographically based bidirectional authentication to protect the integrity of the information in transit.

```
GROUP ID: V-272435
RULE ID: SV-272435r1068144
```

Rationale:

Server-to-server (zone transfer) transactions are provided by TSIG, which enforces mutual server authentication using a key that is unique to each server pair (TSIG), thus uniquely identifying the other server. DNS does perform server authentication when TSIG is used, but this authentication is transactional in nature (each transaction has its own authentication performed).

Enforcing mutually authenticated communication sessions during zone transfers provides the assurance that only authorized servers are requesting and receiving DNS zone data. Without authenticating devices, unidentified or unknown devices may be introduced, thereby facilitating malicious activity.

Failure to properly implement transactional security may have significant effects on the overall security of the DNS infrastructure. The lack of mutual authentication between name servers during a DNS transaction would allow a threat actor to launch a Man-In-The-Middle attack against the DNS infrastructure. This attack could lead to unauthorized DNS zone data being introduced, resulting in network traffic being redirected to a rogue site.

Satisfies: SRG-APP-000439-DNS-000063, SRG-APP-000394-DNS-000049, SRG-APP-000395-DNS-000050, SRG-APP-000440-DNS-000065

Audit:

If zone transfers are disabled with the "allow-transfer { none; };" directive, this is Not Applicable.

Verify that the BIND 9.x server is configured to uniquely identify a name server before responding to a zone transfer.

Inspect the "named.conf" file for the presence of TSIG key statements:

On the primary name server, this is an example of a configured key statement:

```
key tsig_example. {
algorithm hmac-SHA1;
include "tsig-example.key";
};

zone "disa.mil" {
type Primary;
file "db.disa.mil";
allow-transfer { key tsig_example.; };
};
```

On the secondary name server, this is an example of a configured key statement:

```
key tsig_example. {
algorithm hmac-SHA1;
include "tsig-example.key";
};

server <ip_address> {
keys { tsig_example };
};

zone "disa.mil" {
type Secondary;
Primarys { <ip_address>; };
file "db.disa.mil";
};
```

If a primary name server does not have a key defined in the "allow-transfer" block, this is a finding.

If a secondary name server does not have a server statement that contains a "keys" sub statement, this is a finding.

Remediation:

Configure the BIND 9.x server to use TSIG keys.

Add a key statement to the "named.conf" file for TSIG that is being used:

```
key tsig_example. {
algorithm hmac-SHA1;
include "tsig-example.key";
};
```

Add key statements to the allow-transfer statements on a primary name server:

```
allow-transfer { key tsig_example.; };

Add key statements to the server statements on a secondary name server:

server <ip_address> {
keys { tsig_example };
};
```

Restart the BIND 9.x process.

Additional Information:

CCI-002418 Protect the confidentiality and/or integrity of transmitted information.

- NIST SP 800-53 Revision 4::SC-8
- NIST SP 800-53 Revision 5::SC-8

CCI-001958 Authenticate organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection.

- NIST SP 800-53 Revision 4::IA-3
- NIST SP 800-53 Revision 5::IA-3

CCI-001967 Authenticate organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection using bidirectional authentication that is cryptographically based.

- NIST SP 800-53 Revision 4::IA-3 (1)
- NIST SP 800-53 Revision 5::IA-3 (1)

CCI-002421 Implement cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission.

- NIST SP 800-53 Revision 4::SC-8 (1)
- NIST SP 800-53 Revision 5::SC-8 (1)

1.73 BIND-9X-002050 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

A BIND 9.x server must implement NIST FIPS-validated cryptography for provisioning digital signatures and generating cryptographic hashes.

```
GROUP ID: V-272436
RULE ID: SV-272436r1082281
```

Rationale:

Use of weak or untested encryption algorithms undermines the purposes of using encryption to protect data. The application must implement cryptographic modules adhering to the higher standards approved by the federal government since this provides assurance they have been tested and validated.

Audit:

Verify that the DNSSEC and TSIG keys used by the BIND 9.x implementation are FIPS 180-3 compliant.

If the server is in a classified network, the DNSSEC portion of the requirement is Not Applicable.

DNSSEC keys:

Inspect the "named.conf" file and identify all of the DNSSEC signed zone files:

```
zone "example.com" {
file "signed_zone_file";
};
```

For each signed zone file identified, inspect the file for the "DNSKEY" records:

```
86400 DNSKEY 257 3 8 (
<KEY HASH>
) ; KSK;
86400 DNSKEY 256 3 8 (
<KEY HASH>
) ; ZSK;
```

The fifth field in the above example identifies what algorithm was used to create the DNSKEY.

If the fifth field the KSK DNSKEY is less than "8" (SHA256), this is a finding.

If the algorithm used to create the ZSK is less than "8" (SHA256), this is a finding.

TSIG keys:

Inspect the "named.conf" file and identify all of the TSIG key statements:

```
key tsig_example. {
algorithm hmac-SHA256;
include "tsig-example.key";
};
```

If each key statement does not use "hmac-SHA256" or a stronger algorithm, this is a finding.

Remediation:

Create new DNSSEC and TSIG keys using a FIPS 180-3 approved cryptographic algorithm that meets or exceeds the strength of SHA-256.

Additional Information:

CCI-002450 Implement organization-defined types of cryptography for each specified cryptography use.

- NIST SP 800-53 Revision 4::SC-13
- NIST SP 800-53 Revision 5::SC-13 b

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	BIND-9X-001010 (Manual)	☐	☐
1.2	BIND-9X-001020 (Manual)	☐	☐
1.3	BIND-9X-001030 (Manual)	☐	☐
1.4	BIND-9X-001040 (Manual)	☐	☐
1.5	BIND-9X-001050 (Manual)	☐	☐
1.6	BIND-9X-001060 (Manual)	☐	☐
1.7	BIND-9X-001070 (Manual)	☐	☐
1.8	BIND-9X-001110 (Manual)	☐	☐
1.9	BIND-9X-001140 (Manual)	☐	☐
1.10	BIND-9X-001150 (Manual)	☐	☐
1.11	BIND-9X-001170 (Manual)	☐	☐
1.12	BIND-9X-001180 (Manual)	☐	☐
1.13	BIND-9X-001190 (Manual)	☐	☐
1.14	BIND-9X-001200 (Manual)	☐	☐
1.15	BIND-9X-001210 (Manual)	☐	☐
1.16	BIND-9X-001220 (Manual)	☐	☐
1.17	BIND-9X-001230 (Manual)	☐	☐
1.18	BIND-9X-001240 (Manual)	☐	☐
1.19	BIND-9X-001250 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	BIND-9X-001260 (Manual)	☐	☐
1.21	BIND-9X-001270 (Manual)	☐	☐
1.22	BIND-9X-001280 (Manual)	☐	☐
1.23	BIND-9X-001290 (Manual)	☐	☐
1.24	BIND-9X-001300 (Manual)	☐	☐
1.25	BIND-9X-001310 (Manual)	☐	☐
1.26	BIND-9X-001320 (Manual)	☐	☐
1.27	BIND-9X-001340 (Manual)	☐	☐
1.28	BIND-9X-001350 (Manual)	☐	☐
1.29	BIND-9X-001360 (Manual)	☐	☐
1.30	BIND-9X-001370 (Manual)	☐	☐
1.31	BIND-9X-001380 (Manual)	☐	☐
1.32	BIND-9X-001390 (Manual)	☐	☐
1.33	BIND-9X-001400 (Manual)	☐	☐
1.34	BIND-9X-001410 (Manual)	☐	☐
1.35	BIND-9X-001420 (Manual)	☐	☐
1.36	BIND-9X-001430 (Manual)	☐	☐
1.37	BIND-9X-001470 (Manual)	☐	☐
1.38	BIND-9X-001480 (Manual)	☐	☐
1.39	BIND-9X-001490 (Manual)	☐	☐
1.40	BIND-9X-001500 (Manual)	☐	☐
1.41	BIND-9X-001510 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.42	BIND-9X-001520 (Manual)	☐	☐
1.43	BIND-9X-001530 (Manual)	☐	☐
1.44	BIND-9X-001540 (Manual)	☐	☐
1.45	BIND-9X-001550 (Manual)	☐	☐
1.46	BIND-9X-001560 (Manual)	☐	☐
1.47	BIND-9X-001570 (Manual)	☐	☐
1.48	BIND-9X-001580 (Manual)	☐	☐
1.49	BIND-9X-001590 (Manual)	☐	☐
1.50	BIND-9X-001600 (Manual)	☐	☐
1.51	BIND-9X-001610 (Manual)	☐	☐
1.52	BIND-9X-001620 (Manual)	☐	☐
1.53	BIND-9X-001630 (Manual)	☐	☐
1.54	BIND-9X-001650 (Manual)	☐	☐
1.55	BIND-9X-001660 (Manual)	☐	☐
1.56	BIND-9X-001680 (Manual)	☐	☐
1.57	BIND-9X-001690 (Manual)	☐	☐
1.58	BIND-9X-001700 (Manual)	☐	☐
1.59	BIND-9X-001720 (Manual)	☐	☐
1.60	BIND-9X-001740 (Manual)	☐	☐
1.61	BIND-9X-001750 (Manual)	☐	☐
1.62	BIND-9X-001770 (Manual)	☐	☐
1.63	BIND-9X-001780 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.64	BIND-9X-001830 (Manual)	☐	☐
1.65	BIND-9X-001840 (Manual)	☐	☐
1.66	BIND-9X-001850 (Manual)	☐	☐
1.67	BIND-9X-001890 (Manual)	☐	☐
1.68	BIND-9X-001900 (Manual)	☐	☐
1.69	BIND-9X-001910 (Manual)	☐	☐
1.70	BIND-9X-001920 (Manual)	☐	☐
1.71	BIND-9X-001950 (Manual)	☐	☐
1.72	BIND-9X-002010 (Manual)	☐	☐
1.73	BIND-9X-002050 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Sep 11, 2025	1.0.0	Initial CIS Release