CIS VMware vSphere 8.0 vCenter Appliance PostgreSQL STIG Benchmark

v1.0.0 – 04-02-2025

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

Overview

® members.

Target Technology Details

VMware vSphere 8.0 vCenter Appliance PostgreSQL Secure Technical Implementation Guide (STIG)

Version: 2 Release: 2 Benchmark

Date: 02 Apr 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 VMware vSphere 8.0 vCenter Appliance PostgreSQL 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 VMware vSphere 8.0 vCenter Appliance PostgreSQL

Recommendations

1 STIG RULES

VMware vSphere

VMware vSphere 8.0 vCenter Appliance PostgreSQL Secure Technical Implementation Guide (STIG)

Version: 2 Release: 2 Benchmark

Date: 02 Apr 2025

CLASSIFICATION unclassified

1.1 VCPG-80-000001 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter PostgreSQL service must limit the number of concurrent sessions.

```
GROUP ID: V-259166
RULE ID: SV-259166r960735
```

Rationale:

Database management includes the ability to control the number of users and user sessions utilizing a database management system (DBMS). Unlimited concurrent connections to the DBMS could allow a successful denial-of-service (DoS) attack by exhausting connection resources, and a system can also fail or be degraded by an overload of legitimate users. Limiting the number of concurrent sessions per user is helpful in reducing these risks.

VMware Postgres as deployed on the vCenter Service Appliance (VCSA) comes preconfigured with a "max_connections" limit that is appropriate for all tested, supported scenarios. The out-of-the-box configuration is dynamic, based on a lower limit plus allowances for the resources assigned to VCSA and the deployment size. However, this number will always be between 100 and 1000 (inclusive).

Audit:

At the command prompt, run the following command:

/opt/vmware/vpostgres/current/bin/psql -U postgres -A -t -c "SHOW max_connections;"

If the returned number is not greater than or equal to 100 and less than or equal to 1000, this is a finding.

Remediation:

At the command prompt, run the following command:

vmon-cli --restart vmware-vpostgres

Note: Restarting the service runs the "pg_tuning" script that will configure "max_connections" to the appropriate value based on the allocated memory for vCenter.

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 VCPG-80-000005 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter PostgreSQL service must enable "pgaudit" to provide audit record generation capabilities.

```
GROUP ID: V-259167
RULE ID: SV-259167r960879
```

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.

Audit records can be generated from various components within the database management system (DBMS) (e.g., process, module). Certain specific application functionalities may be audited as well. 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.

DOD has defined the list of events for which the DBMS 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.

Organizations may define additional events requiring continuous or ad hoc auditing.

Audit:

At the command prompt, run the following command:

/opt/vmware/vpostgres/current/bin/psql -U postgres -A -t -c "SHOW shared_preload_libraries;"

Example result:

health_status_worker,pg_stat_statements,pgaudit

If the output from the command does not include pgaudit, this is a finding.

Remediation:

A script is included with vCenter to generate a PostgreSQL STIG configuration.

At the command prompt, run the following commands:

chmod +x /opt/vmware/vpostgres/current/bin/vmw_vpg_config/vmw_vpg_config.py /opt/vmware/vpostgres/current/bin/vmw_vpg_config/vmw_vpg_config.py --action stig_enable --pg-data-dir /storage/db/vpostgres chmod -x /opt/vmware/vpostgres/current/bin/vmw_vpg_config/vmw_vpg_config.py

Restart the PostgreSQL service by running the following command:

vmon-cli --restart vmware-vpostgres

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

1.3 VCPG-80-000006 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter PostgreSQL service configuration files must not be accessible by unauthorized users.

```
GROUP ID: V-259168
RULE ID: SV-259168r960882
```

Rationale:

Without the capability to restrict which roles and individuals can select which events are audited, unauthorized personnel may be able to prevent or interfere with the auditing of critical events.

Suppression of auditing could permit an adversary to evade detection.

Misconfigured audits can degrade the system's performance by overwhelming the audit log. Misconfigured audits may also make it more difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Satisfies: SRG-APP-000090-DB-000065, SRG-APP-000121-DB-000202, SRG-APP-000122-DB-000203, SRG-APP-000123-DB-000204, SRG-APP-000380-DB-000360

Audit:

At the command prompt, run the following command:

find /storage/db/vpostgres/*conf* -xdev -type f -a '(' -not -perm 600 -o -not -user vpostgres -o -not -group vpgmongrp ')' -exec ls -ld {} ;

If any files are returned, this is a finding.

Remediation:

At the command prompt, run the following commands:

chmod 600 chown vpostgres:vpgmongrp

Note: Replace with the file that has incorrect permissions.

Additional Information:

CCI-000171 Allow organization-defined personnel or roles to select the event types that are to be logged by specific components of the system.

- NIST SP 800-53::AU-12 b
- NIST SP 800-53A::AU-12.1 (iii)

- NIST SP 800-53 Revision 4::AU-12 b
- NIST SP 800-53 Revision 5::AU-12 b

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001495 Protect audit tools from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001813 Enforce access restrictions using organization-defined mechanisms.

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

1.4 VCPG-80-000010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter PostgreSQL service must produce logs containing sufficient information to establish what type of events occurred.

```
GROUP ID: V-259171
RULE ID: SV-259171r960891
```

Rationale:

Information system auditing capability is critical for accurate forensic analysis. Without establishing what type of event occurred, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit record content that may be necessary to satisfy the requirement of this policy includes, for example, time stamps, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

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.

Database software is capable of a range of actions on data stored within the database. It is important, for accurate forensic analysis, to know exactly what actions were performed. This requires specific information regarding the event type an audit record is referring to. If event type information is not recorded and stored with the audit record, the record itself is of very limited use.

Satisfies: SRG-APP-000095-DB-000039, SRG-APP-000096-DB-000040, SRG-APP-000097-DB-000041, SRG-APP-000098-DB-000042, SRG-APP-000099-DB-000043, SRG-APP-000100-DB-000201, SRG-APP-000101-DB-000044, SRG-APP-000375-DB-000323

Audit:

At the command prompt, run the following command:

/opt/vmware/vpostgres/current/bin/psql -U postgres -A -t -c "SHOW log_line_prefix;"

Expected result:

%m %c %x %d %u %r %p %l

If the output does not include each option in the expected result, this is a finding.

Remediation:

A script is included with vCenter to generate a PostgreSQL STIG configuration.

At the command prompt, run the following commands:

chmod +x /opt/vmware/vpostgres/current/bin/vmw_vpg_config/vmw_vpg_config.py
/opt/vmware/vpostgres/current/bin/vmw_vpg_config/vmw_vpg_config.py --action
stig_enable --pg-data-dir /storage/db/vpostgres chmod -x
/opt/vmware/vpostgres/current/bin/vmw_vpg_config/vmw_vpg_config.py

Restart the PostgreSQL service by running the following command:

vmon-cli --restart vmware-vpostgres

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

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

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

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-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

CCI-001487 Ensure that audit records containing information that establishes the identity of any individuals, subjects, or objects/entities associated with 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 f

CCI-001889 Record time stamps for audit records that meet organization-defined granularity of time measurement.

- NIST SP 800-53 Revision 4::AU-8 b
- NIST SP 800-53 Revision 5::AU-8 b

1.5 VCPG-80-000007 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter PostgreSQL service must generate audit records.

```
GROUP ID: V-259169
RULE ID: SV-259169r1067578
```

Rationale:

Under some circumstances, it may be useful to monitor who/what is reading privilege/permission/role information. Therefore, it must be possible to configure auditing to do this. Database management systems (DBMS) typically make such information available through views or functions.

This requirement addresses explicit requests for privilege/permission/role membership information. It does not refer to the implicit retrieval of privileges/permissions/role memberships that PostgreSQL continually performs to determine if any and every action on the database is permitted.

Satisfies: SRG-APP-000091-DB-000066, SRG-APP-000091-DB-000325, SRG-APP-000492-DB-000332, SRG-APP-000492-DB-000333, SRG-APP-000495-DB-000326, SRG-APP-000495-DB-000327, SRG-APP-000495-DB-000328, SRG-APP-000495-DB-000329, SRG-APP-000496-DB-000334, SRG-APP-000496-DB-000335, SRG-APP-000499-DB-000330, SRG-APP-000499-DB-000331, SRG-APP-000501-DB-000336, SRG-APP-000501-DB-000337, SRG-APP-000504-DB-000354, SRG-APP-000504-DB-000355, SRG-APP-000507-DB-000356, SRG-APP-000507-DB-000357

Audit:

At the command prompt, run the following commands:

/opt/vmware/vpostgres/current/bin/psql -U postgres -A -t -c "SHOW pgaudit.log;"

If the "pgaudit.log" setting is not configured to "all, -misc, -read", this is a finding.

Remediation:

A script is included with vCenter to generate a PostgreSQL STIG configuration.

At the command prompt, run the following commands:

chmod +x /opt/vmware/vpostgres/current/bin/vmw_vpg_config/vmw_vpg_config.py /opt/vmware/vpostgres/current/bin/vmw_vpg_config/vmw_vpg_config.py --action stig_enable --pg-data-dir /storage/db/vpostgres chmod -x /opt/vmware/vpostgres/current/bin/vmw_vpg_config/vmw_vpg_config.py

Note: If this has already been run previously it does not need to be run again.

Navigate to and edit the /storage/db/vpostgres/stig.conf file.

Add or update the following settings:

pgaudit.log = 'all, -misc, -read' pgaudit.log_catalog = off pgaudit.log_parameter = off pgaudit.log_relation = off pgaudit.log_statement = off

Remove the following settings:

pgaudit.log_level = log

Restart the PostgreSQL service by running the following command:

vmon-cli --restart vmware-vpostgres

Additional Information:

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

1.6 VCPG-80-000009 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter PostgreSQL service must initiate session auditing upon startup.

```
GROUP ID: V-259170
RULE ID: SV-259170r960888
```

Rationale:

Session auditing is for use when a user's activities are under investigation. To be sure of capturing all activity during those periods when session auditing is in use, it needs to be in operation for the whole time the database management system (DBMS) is running.

Audit:

At the command prompt, run the following command:

/opt/vmware/vpostgres/current/bin/psql -U postgres -A -t -c "SHOW log_destination;"

Example result:

stderr

If "log_destination" is not set to "stderr" or "syslog", this is a finding.

Remediation:

A script is included with vCenter to generate a PostgreSQL STIG configuration.

At the command prompt, run the following commands:

chmod +x /opt/vmware/vpostgres/current/bin/vmw_vpg_config/vmw_vpg_config.py /opt/vmware/vpostgres/current/bin/vmw_vpg_config/vmw_vpg_config.py --action stig_enable --pg-data-dir /storage/db/vpostgres chmod -x /opt/vmware/vpostgres/current/bin/vmw_vpg_config/vmw_vpg_config.py

Restart the PostgreSQL service by running the following command:

vmon-cli --restart vmware-vpostgres

Additional Information:

CCI-001464 Initiates session audits automatically at system start-up.

- NIST SP 800-53::AU-14 (1)
- NIST SP 800-53A::AU-14 (1).1

- NIST SP 800-53 Revision 4::AU-14 (1)
- NIST SP 800-53 Revision 5::AU-14 (1)

1.7 VCPG-80-000020 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter PostgreSQL service must be configured to protect log files from unauthorized access.

```
GROUP ID: V-259172
RULE ID: SV-259172r960930
```

Rationale:

If audit data were to become compromised, then competent forensic analysis and discovery of the true source of potentially malicious system activity is difficult, if not impossible, to achieve. In addition, access to audit records provides information an attacker could potentially use to his or her advantage.

To ensure the veracity of audit data, the information system and/or the application must protect audit information from any and all unauthorized access. This includes read, write, copy, etc.

Satisfies: SRG-APP-000118-DB-000059, SRG-APP-000119-DB-000060, SRG-APP-000120-DB-000061

Audit:

Verify the default log file permissions and permissions on existing log files.

At the command prompt, run the following command:

/opt/vmware/vpostgres/current/bin/psql -U postgres -A -t -c "SHOW log_file_mode;"

Expected result:

0600

If "log_file_mode" is not set to "0600", this is a finding.

At the command prompt, run the following command:

find /var/log/vmware/vpostgres/* -xdev -type f -a '(' -not -perm 600 -o -not -user vpostgres -o -not -group vpgmongrp ')' -exec ls -ld {} ;

If any files are returned, this is a finding.

Remediation:

A script is included with vCenter to generate a PostgreSQL STIG configuration.

At the command prompt, run the following commands:

chmod +x /opt/vmware/vpostgres/current/bin/vmw_vpg_config/vmw_vpg_config.py /opt/vmware/vpostgres/current/bin/vmw_vpg_config/vmw_vpg_config.py --action stig_enable --pg-data-dir /storage/db/vpostgres chmod -x /opt/vmware/vpostgres/current/bin/vmw_vpg_config/vmw_vpg_config.py

Restart the PostgreSQL service by running the following command:

vmon-cli --restart vmware-vpostgres

At the command prompt, run the following commands:

chmod 600 chown vpostgres:vpgmongrp

Note: Replace with the file that has incorrect permissions.

Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

1.8 VCPG-80-000032 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter PostgreSQL service must not load unused database components, software, and database objects.

```
GROUP ID: V-259173
RULE ID: SV-259173r960963
```

Rationale:

Information systems 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 (e.g., key missions, functions).

It is detrimental for software products to provide, or install by default, functionality exceeding requirements or mission objectives.

Database management systems (DBMS) must adhere to the principles of least functionality by providing only essential capabilities.

Satisfies: SRG-APP-000141-DB-000091, SRG-APP-000141-DB-000093

Audit:

At the command prompt, run the following command:

/opt/vmware/vpostgres/current/bin/psql -U postgres -A -t -c "select * from pg_extension where extname != 'plpgsql'"

If any extensions are output, this is a finding.

Remediation:

At the command prompt, run the following command:

```
$ /opt/vmware/vpostgres/current/bin/psql -U postgres -c  "DROP EXTENSION
<extension name>"
```

Note: It is recommended that plpgsql not be removed.

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)

- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

1.9 VCPG-80-000035 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter PostgreSQL service must be configured to use an authorized port.

```
GROUP ID: V-259174
RULE ID: SV-259174r1043177
```

Rationale:

In order 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/services 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 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.

Database Management Systems using ports, protocols, and services deemed unsafe are open to attack through those ports, protocols, and services. This can allow unauthorized access to the database and through the database to other components of the information system.

Satisfies: SRG-APP-000142-DB-000094, SRG-APP-000383-DB-000364

Audit:

At the command prompt, run the following command:

```
$ /opt/vmware/vpostgres/current/bin/psql -U postgres -A -t -c "SHOW port;"
```

Expected result:

5432

If the output does not match the expected result, this is a finding.

Remediation:

A script is included with vCenter to generate a PostgreSQL STIG configuration.

At the command prompt, run the following commands:

chmod +x /opt/vmware/vpostgres/current/bin/vmw_vpg_config/vmw_vpg_config.py /opt/vmware/vpostgres/current/bin/vmw_vpg_config/vmw_vpg_config.py --action stig_enable --pg-data-dir /storage/db/vpostgres chmod -x /opt/vmware/vpostgres/current/bin/vmw_vpg_config/vmw_vpg_config.py

Restart the PostgreSQL service by running the following command:

vmon-cli --restart vmware-vpostgres

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

CCI-001762 Disable or remove organization-defined functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure.

- NIST SP 800-53 Revision 4::CM-7 (1) (b)
- NIST SP 800-53 Revision 5::CM-7 (1) (b)

1.10 VCPG-80-000036 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter PostgreSQL service must require authentication on all connections.

```
GROUP ID: V-259175
RULE ID: SV-259175r1051115
```

Rationale:

To assure accountability and prevent unauthenticated access, organizational users must be identified and authenticated to prevent potential misuse and compromise of the system.

Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors). Organizational users (and any processes acting on behalf of users) must be uniquely identified and authenticated for all accesses, except the following:

(i) Accesses explicitly identified and documented by the organization. Organizations document specific user actions that can be performed on the information system without identification or authentication; and (ii) Accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals using shared accounts, for detailed accountability of individual activity.

Satisfies: SRG-APP-000148-DB-000103, SRG-APP-000172-DB-000075

Audit:

At the command prompt, run the following command:

grep -v "^" /storage/db/vpostgres/pg_hba.conf |grep '\S'

If any lines are returned contain "trust" or "password" as an auth-method, this is a finding.

Remediation:

Navigate to and open:

/storage/db/vpostgres/pg_hba.conf

Find and update any line that has a method of "trust" or "password" in the far-right column.

A correct, typical line will look like the below:

TYPE DATABASE USER ADDRESS METHOD local VCDB vpxd peer map=vcdb

Restart the PostgreSQL service by running the following command:

vmon-cli --restart vmware-vpostgres

Additional Information:

CCI-000197 For password-based authentication, transmit passwords only over cryptographically-protected channels.

- NIST SP 800-53::IA-5 (1) (c)
- NIST SP 800-53A::IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4::IA-5 (1) (c)
- NIST SP 800-53 Revision 5::IA-5 (1) (c)

CCI-000764 Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

- NIST SP 800-53::IA-2
- NIST SP 800-53A::IA-2.1
- NIST SP 800-53 Revision 4::IA-2
- NIST SP 800-53 Revision 5::IA-2

1.11 VCPG-80-000038 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The vCenter PostgreSQL service must encrypt passwords for user authentication.

```
GROUP ID: V-259176
RULE ID: SV-259176r1015952
```

Rationale:

The DOD standard for authentication is DOD-approved PKI certificates.

Authentication based on User ID and Password may be used only when it is not possible to employ a PKI certificate and requires AO approval.

In such cases, database passwords stored in clear text, using reversible encryption, or using unsalted hashes would be vulnerable to unauthorized disclosure. Database passwords must always be in the form of one-way, salted hashes when stored internally or externally to the database management system (DBMS).

Audit:

At the command prompt, run the following command:

```
$ /opt/vmware/vpostgres/current/bin/psql -U postgres -A -t -c "SHOW
password_encryption;"
```

Expected result:

scram-sha-256

If the output does not match the expected result, this is a finding.

Note: Prior to Update 2, "md5" is the expected result.

Remediation:

A script is included with vCenter to generate a PostgreSQL STIG configuration.

At the command prompt, run the following commands:

chmod +x /opt/vmware/vpostgres/current/bin/vmw_vpg_config/vmw_vpg_config.py /opt/vmware/vpostgres/current/bin/vmw_vpg_config/vmw_vpg_config.py --action stig_enable --pg-data-dir /storage/db/vpostgres chmod -x /opt/vmware/vpostgres/current/bin/vmw_vpg_config/vmw_vpg_config.py

Restart the PostgreSQL service by running the following command:

vmon-cli --restart vmware-vpostgres

Additional Information:

CCI-004062 For password-based authentication, store passwords using an approved salted key derivation function, preferably using a keyed hash.

- NIST SP 800-53 Revision 5::IA-5 (1) (d)

CCI-000196 The information system, for password-based authentication, stores only cryptographically-protected passwords.

- NIST SP 800-53::IA-5 (1) (c)
- NIST SP 800-53A::IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4::IA-5 (1) (c)

1.12 VCPG-80-000051 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter PostgreSQL service must write log entries to disk prior to returning operation success or failure.

```
GROUP ID: V-259179
RULE ID: SV-259179r961125
```

Rationale:

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 system state information helps to facilitate system restart and return to the operational mode of the organization with less disruption of mission/business processes.

Aggregating log writes saves on performance but leaves a window for log data loss. The logging system inside PostgreSQL is capable of writing logs to disk, fully and completely before the associated operation is returned to the client. This ensures that database activity is always captured, even in the event of a system crash during or immediately after a given operation.

Audit:

At the command prompt, run the following command:

/opt/vmware/vpostgres/current/bin/psql -U postgres -A -t -c "SELECT name,setting FROM pg_settings WHERE name IN ('fsync','full_page_writes','synchronous_commit');"

Expected result:

fsync | on full_page_writes | on synchronous_commit | on

If the output does not match the expected result, this is a finding.

Remediation:

A script is included with vCenter to generate a PostgreSQL STIG configuration.

At the command prompt, run the following commands:

chmod +x /opt/vmware/vpostgres/current/bin/vmw_vpg_config/vmw_vpg_config.py /opt/vmware/vpostgres/current/bin/vmw_vpg_config/vmw_vpg_config.py --action stig_enable --pg-data-dir /storage/db/vpostgres chmod -x /opt/vmware/vpostgres/current/bin/vmw_vpg_config/vmw_vpg_config.py

Restart the PostgreSQL service by running the following command:

vmon-cli --restart vmware-vpostgres

Additional Information:

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

1.13 VCPG-80-000060 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter PostgreSQL service must provide nonprivileged users with minimal error information.

```
GROUP ID: V-259180
RULE ID: SV-259180r961167
```

Rationale:

Any DBMS or associated application providing too much information in error messages on the screen or printout risks compromising the data and security of the system. The structure and content of error messages need to contain the minimal amount of information.

Databases can inadvertently provide a wealth of information to an attacker through improperly handled error messages. In addition to sensitive business or personal information, database errors can provide host names, IP addresses, usernames, and other system information not required for troubleshooting but very useful to someone targeting the system.

Satisfies: SRG-APP-000266-DB-000162, SRG-APP-000267-DB-000163

Audit:

At the command prompt, run the following command:

/opt/vmware/vpostgres/current/bin/psql -U postgres -A -t -c "SHOW client_min_messages;"

Expected result:

error

If the output does not match the expected result, this is a finding.

Remediation:

A script is included with vCenter to generate a PostgreSQL STIG configuration.

At the command prompt, run the following commands:

chmod +x /opt/vmware/vpostgres/current/bin/vmw_vpg_config/vmw_vpg_config.py /opt/vmware/vpostgres/current/bin/vmw_vpg_config/vmw_vpg_config.py --action stig_enable --pg-data-dir /storage/db/vpostgres chmod -x /opt/vmware/vpostgres/current/bin/vmw_vpg_config/vmw_vpg_config.py

Restart the PostgreSQL service by running the following command:

vmon-cli --restart vmware-vpostgres

Additional Information:

CCI-001312 Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited.

- NIST SP 800-53::SI-11 b
- NIST SP 800-53A::SI-11.1 (iii)
- NIST SP 800-53 Revision 4::SI-11 a
- NIST SP 800-53 Revision 5::SI-11 a

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53::SI-11 c
- NIST SP 800-53A::SI-11.1 (iv)
- NIST SP 800-53 Revision 4::SI-11 b
- NIST SP 800-53 Revision 5::SI-11 b

1.14 VCPG-80-000070 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter PostgreSQL service must have log collection enabled.

```
GROUP ID: V-259181
RULE ID: SV-259181r1015953
```

Rationale:

Without the ability to centrally manage the content captured in the audit records, identification, troubleshooting, and correlation of suspicious behavior would be difficult and could lead to a delayed or incomplete analysis of an ongoing attack.

The content captured in audit records must be managed from a central location (necessitating automation). Centralized management of audit records and logs provides for efficiency in maintenance and management of records, as well as the backup and archiving of those records.

Satisfies: SRG-APP-000356-DB-000314, SRG-APP-000381-DB-000361

Audit:

At the command prompt, run the following command:

/opt/vmware/vpostgres/current/bin/psql -U postgres -A -t -c "SHOW logging_collector;"

Expected result:

on

If the output does not match the expected result, this is a finding.

Remediation:

A script is included with vCenter to generate a PostgreSQL STIG configuration.

At the command prompt, run the following commands:

chmod +x /opt/vmware/vpostgres/current/bin/vmw_vpg_config/vmw_vpg_config.py
/opt/vmware/vpostgres/current/bin/vmw_vpg_config/vmw_vpg_config.py --action stig_enable --pg-data-dir /storage/db/vpostgres chmod -x /opt/vmware/vpostgres/current/bin/vmw_vpg_config/vmw_vpg_config.py

Restart the PostgreSQL service by running the following command:

vmon-cli --restart vmware-vpostgres

Additional Information:

CCI-003938 Automatically generate audit records of the enforcement actions.

- NIST SP 800-53 Revision 5::CM-5 (1) (b)

CCI-001814 The Information system supports auditing of the enforcement actions.

- NIST SP 800-53 Revision 4::CM-5 (1)

1.15 VCPG-80-000075 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter PostgreSQL service must use Coordinated Universal Time (UTC) for log timestamps.

```
GROUP ID: V-259182
RULE ID: SV-259182r961443
```

Rationale:

If time stamps are not consistently applied and there is no common time reference, it is difficult to perform forensic analysis.

Time stamps generated by PostgreSQL must include date and time. Time is commonly expressed in UTC, a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC.

Audit:

At the command prompt, run the following command:

/opt/vmware/vpostgres/current/bin/psql -U postgres -A -t -c "SHOW log_timezone;"

Expected result:

UTC

If the output does not match the expected result, this is a finding.

Remediation:

A script is included with vCenter to generate a PostgreSQL STIG configuration.

At the command prompt, run the following commands:

chmod +x /opt/vmware/vpostgres/current/bin/vmw_vpg_config/vmw_vpg_config.py /opt/vmware/vpostgres/current/bin/vmw_vpg_config/vmw_vpg_config.py --action stig_enable --pg-data-dir /storage/db/vpostgres chmod -x /opt/vmware/vpostgres/current/bin/vmw_vpg_config/vmw_vpg_config.py

Restart the PostgreSQL service by running the following command:

vmon-cli --restart vmware-vpostgres

Additional Information:

CCI-001890 Record time stamps for audit records that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

- NIST SP 800-53 Revision 4::AU-8 b
- NIST SP 800-53 Revision 5::AU-8 b

1.16 VCPG-80-000110 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter PostgreSQL service must log all connection attempts.

```
GROUP ID: V-259183
RULE ID: SV-259183r961824
```

Rationale:

For completeness of forensic analysis, it is necessary to track successful and failed attempts to log on to PostgreSQL. Setting "log_connections" to "on" will cause each attempted connection to the server to be logged, as well as successful completion of client authentication.

Satisfies: SRG-APP-000503-DB-000350, SRG-APP-000503-DB-000351, SRG-APP-000506-DB-000353, SRG-APP-000508-DB-000358

Audit:

At the command prompt, run the following command:

/opt/vmware/vpostgres/current/bin/psql -U postgres -A -t -c "SHOW log_connections;"

Expected result:

on

If the output does not match the expected result, this is a finding.

Remediation:

A script is included with vCenter to generate a PostgreSQL STIG configuration.

At the command prompt, run the following commands:

chmod +x /opt/vmware/vpostgres/current/bin/vmw_vpg_config/vmw_vpg_config.py /opt/vmware/vpostgres/current/bin/vmw_vpg_config/vmw_vpg_config.py --action stig_enable --pg-data-dir /storage/db/vpostgres chmod -x /opt/vmware/vpostgres/current/bin/vmw_vpg_config/vmw_vpg_config.py

Restart the PostgreSQL service by running the following command:

vmon-cli --restart vmware-vpostgres

Additional Information:

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

1.17 VCPG-80-000114 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter PostgreSQL service must log all client disconnections.

```
GROUP ID: V-259184
RULE ID: SV-259184r961830
```

Rationale:

Disconnection may be initiated by the user or forced by the system (as in a timeout) or result from a system or network failure. To the greatest extent possible, all disconnections must be logged.

For completeness of forensic analysis, it is necessary to know how long a user's (or other principal's) connection to PostgreSQL lasts. This can be achieved by recording disconnections, in addition to logons/connections, in the audit logs.

Audit:

At the command prompt, run the following command:

/opt/vmware/vpostgres/current/bin/psql -U postgres -A -t -c "SHOW log_disconnections;"

Expected result:

on

If the output does not match the expected result, this is a finding.

Remediation:

A script is included with vCenter to generate a PostgreSQL STIG configuration.

At the command prompt, run the following commands:

chmod +x /opt/vmware/vpostgres/current/bin/vmw_vpg_config/vmw_vpg_config.py /opt/vmware/vpostgres/current/bin/vmw_vpg_config/vmw_vpg_config.py --action stig_enable --pg-data-dir /storage/db/vpostgres chmod -x /opt/vmware/vpostgres/current/bin/vmw_vpg_config/vmw_vpg_config.py

Restart the PostgreSQL service by running the following command:

vmon-cli --restart vmware-vpostgres

Additional Information:

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

1.18 VCPG-80-000122 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter PostgreSQL service must off-load audit data to a separate log management facility.

```
GROUP ID: V-259185
RULE ID: SV-259185r961860
```

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

The database management system (DBMS) may write audit records to database tables, to files in the file system, to other kinds of local repository, or directly to a centralized log management system. Whatever the method used, it must be compatible with off-loading the records to the centralized system.

Audit:

By default there is a vmware-services-vmware-vpostgres.conf rsyslog and vmware-services-vmware-postgres-archiver.conf configuration file that includes the service logs when syslog is configured on vCenter but it must be verified.

At the command prompt, run the following command:

cat /etc/vmware-syslog/vmware-services-vmware-vpostgres.conf

Expected result:

vmware-vpostgres first logs stdout, before loading configuration input(type="imfile" File="/var/log/vmware/vpostgres/serverlog.stdout" Tag="vpostgres-first" Severity="info" Facility="local0") vmware-vpostgres first logs stderr, before loading configuration input(type="imfile" File="/var/log/vmware/vpostgres/serverlog.stderr" Tag="vpostgres-first" Severity="info" Facility="local0") vmware-vpostgres logs input(type="imfile" File="/var/log/vmware/vpostgres/postgresql-*.log" Tag="vpostgres" Severity="info" Facility="local0")

If the output does not match the expected result, this is a finding.

At the command prompt, run the following command:

cat /etc/vmware-syslog/vmware-services-vmware-postgres-archiver.conf

Expected result:

vmware-postgres-archiver stdout log input(type="imfile" File="/var/log/vmware/vpostgres/pg_archiver.log.stdout" Tag="postgres-archiver" Severity="info" Facility="local0") vmware-postgres-archiver stderr log input(type="imfile" File="/var/log/vmware/vpostgres/pg_archiver.log.stderr" Tag="postgres-archiver" Severity="info" Facility="local0")

If the output does not match the expected result, this is a finding.

Remediation:

Navigate to and open:

/etc/vmware-syslog/vmware-services-vmware-vpostgres.conf

Create the file if it does not exist.

Set the contents of the file as follows:

vmware-vpostgres first logs stdout, before loading configuration input(type="imfile" File="/var/log/vmware/vpostgres/serverlog.stdout" Tag="vpostgres-first" Severity="info" Facility="local0") vmware-vpostgres first logs stderr, before loading configuration input(type="imfile" File="/var/log/vmware/vpostgres/serverlog.stderr" Tag="vpostgres-first" Severity="info" Facility="local0") vmware-vpostgres logs input(type="imfile" File="/var/log/vmware/vpostgres/postgresql-*.log" Tag="vpostgres" Severity="info" Facility="local0")

Navigate to and open:

/etc/vmware-syslog/vmware-services-vmware-postgres-archiver.conf

Create the file if it does not exist.

Set the contents of the file as follows:

vmware-postgres-archiver stdout log input(type="imfile" File="/var/log/vmware/vpostgres/pg_archiver.log.stdout" Tag="postgres-archiver" Severity="info" Facility="local0") vmware-postgres-archiver stderr log input(type="imfile" File="/var/log/vmware/vpostgres/pg_archiver.log.stderr" Tag="postgres-archiver" Severity="info" Facility="local0")

Additional Information:

CCI-001851 Transfer audit logs per organization-defined frequency to a different system, system component, or media than the system or system component conducting the logging.

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

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	VCPG-80-000001 (Manual)	☐	☐
1.2	VCPG-80-000005 (Manual)	☐	☐
1.3	VCPG-80-000006 (Manual)	☐	☐
1.4	VCPG-80-000010 (Manual)	☐	☐
1.5	VCPG-80-000007 (Manual)	☐	☐
1.6	VCPG-80-000009 (Manual)	☐	☐
1.7	VCPG-80-000020 (Manual)	☐	☐
1.8	VCPG-80-000032 (Manual)	☐	☐
1.9	VCPG-80-000035 (Manual)	☐	☐
1.10	VCPG-80-000036 (Manual)	☐	☐
1.11	VCPG-80-000038 (Manual)	☐	☐
1.12	VCPG-80-000051 (Manual)	☐	☐
1.13	VCPG-80-000060 (Manual)	☐	☐
1.14	VCPG-80-000070 (Manual)	☐	☐
1.15	VCPG-80-000075 (Manual)	☐	☐
1.16	VCPG-80-000110 (Manual)	☐	☐
1.17	VCPG-80-000114 (Manual)	☐	☐
1.18	VCPG-80-000122 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
09-16-2025	1.0.0	Initial CIS Release