CIS VMware vSphere 8.0 vCenter Appliance User Interface (UI) STIG Benchmark

v1.0.0 – 08-01-2024

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

Target Technology Details

VMware vSphere 8.0 vCenter Appliance User Interface (UI) Secure Technical Implementation Guide (STIG)

Version: 2 Release: 1 Benchmark

Date: 01 Aug 2024

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 User Interface (UI) 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 User Interface (UI)

Recommendations

1 STIG RULES

VMware vSphere

VMware vSphere 8.0 vCenter Appliance User Interface (UI) Secure Technical Implementation Guide (STIG)

Version: 2 Release: 1 Benchmark

Date: 01 Aug 2024

CLASSIFICATION unclassified

1.1 VCUI-80-000001 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter UI service must limit the number of maximum concurrent connections permitted.

```
GROUP ID: V-259104
RULE ID: SV-259104r960735
```

Rationale:

Resource exhaustion can occur when an unlimited number of concurrent requests are allowed on a website, facilitating a denial-of-service attack. Unless the number of requests is controlled, the web server can consume enough system resources to cause a system crash.

Mitigating this kind of attack will include limiting the number of concurrent HTTP/HTTPS requests. In Tomcat, each incoming request requires a thread for the duration of that request. If more simultaneous requests are received than can be handled by the currently available request processing threads, additional threads will be created up to the value of the maxThreads attribute.

Satisfies: SRG-APP-000001-AS-000001, SRG-APP-000435-AS-000163

Audit:

At the command prompt, run the following command:

xmllint --xpath '/Server/Service/Connector[@port="${http.port}"]/@maxThreads' /usr/lib/vmware-vsphere-ui/server/conf/server.xml

Expected result:

maxThreads="800"

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

Remediation:

Navigate to and open:

/usr/lib/vmware-vsphere-ui/server/conf/server.xml

Navigate to the <Connector> node and configure with the value "maxThreads="800"".

Restart the service with the following command:

vmon-cli --restart vsphere-ui

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

CCI-002385 Protect against or limit the effects of organization-defined types of denial-of-service events.

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

1.2 VCUI-80-000005 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter UI service cookies must have secure flag set.

```
GROUP ID: V-259105
RULE ID: SV-259105r960792
```

Rationale:

The secure flag is an option that can be set by the application server when sending a new cookie to the user within an HTTP Response. The purpose of the secure flag is to prevent cookies from being observed by unauthorized parties due to the transmission of a cookie in clear text.

By setting the secure flag, the browser will prevent the transmission of a cookie over an unencrypted channel.

Audit:

At the command prompt, run the following command:

xmllint --format /usr/lib/vmware-vsphere-ui/server/conf/web.xml | sed 's/xmlns=".*"//g' | xmllint --xpath '/web-app/session-config/cookie-config/secure' -

Expected result:

true

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

Remediation:

Navigate to and open:

/usr/lib/vmware-vsphere-ui/server/conf/web.xml

Navigate to the node and configure the setting as follows:

Restart the service with the following command:

vmon-cli --restart vsphere-ui

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

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

1.3 VCUI-80-000013 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter UI service must initiate session logging upon startup.

```
GROUP ID: V-259106
RULE ID: SV-259106r960888
```

Rationale:

Logging must be started as soon as possible when a service starts and as late as possible when a service is stopped. Many forms of suspicious actions can be detected by analyzing logs for unexpected service starts and stops. Also, by starting to log immediately after a service starts, it becomes more difficult for suspicious activity to go unlogged.

Audit:

At the command prompt, run the following command:

grep StreamRedirectFile /etc/vmware/vmware-vmon/svcCfgfiles/vsphere-ui.json

Expected output:

"StreamRedirectFile" : "%VMWARE_LOG_DIR%/vmware/vsphere-ui/logs/vsphere-ui-runtime.log",

If no log file is specified for the "StreamRedirectFile" setting, this is a finding.

Remediation:

Navigate to and open:

/etc/vmware/vmware-vmon/svcCfgfiles/vsphere-ui.json

Below the last line of the "PreStartCommandArg" block, add the following line:

"StreamRedirectFile" : "%VMWARE_LOG_DIR%/vmware/vsphere-ui/logs/vsphere-ui-runtime.log",

Restart the service with the following command:

vmon-cli --restart vsphere-ui

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)

1.4 VCUI-80-000014 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter UI service must produce log records containing sufficient information regarding event details.

```
GROUP ID: V-259107
RULE ID: SV-259107r960891
```

Rationale:

Remote access can be exploited by an attacker to compromise the server. By recording all remote access activities, it will be possible to determine the attacker's location, intent, and degree of success.

Tomcat can be configured with an "AccessLogValve", a component that can be inserted into the request processing pipeline to provide robust access logging. The "AccessLogValve" creates log files in the same format as those created by standard web servers. When "AccessLogValve" is properly configured, log files will contain all the forensic information necessary in the case of a security incident.

Satisfies: SRG-APP-000095-AS-000056, SRG-APP-000016-AS-000013, SRG-APP-000080-AS-000045, SRG-APP-000089-AS-000050, SRG-APP-000090-AS-000051, SRG-APP-000091-AS-000052, SRG-APP-000096-AS-000059, SRG-APP-000097-AS-000060, SRG-APP-000098-AS-000061, SRG-APP-000099-AS-000062, SRG-APP-000100-AS-000063, SRG-APP-000343-AS-000030, SRG-APP-000375-AS-000211, SRG-APP-000495-AS-000220, SRG-APP-000499-AS-000224, SRG-APP-000503-AS-000228

Audit:

At the command prompt, run the following command:

xmllint --xpath '/Server/Service/Engine/Host/Valve[@className="org.apache.catalina.valves.AccessLogValve"]/@pattern' /usr/lib/vmware-vsphere-ui/server/conf/server.xml

Example result:

pattern="%h %{x-forwarded-for}i %l %u %t "%r" %s %b %{hashedClientId}s %{hashedRequestId}r %I %D"

Required elements:

%h %{X-Forwarded-For}i %l %t %u "%r" %s %b

If the log pattern does not contain the required elements in any order, this is a finding.

Remediation:

Navigate to and open:

/usr/lib/vmware-vsphere-ui/server/conf/server.xml

Inside the <Host> node, find the "AccessLogValve" <Valve> node and replace the "pattern" element as follows:

pattern="%h %{x-forwarded-for}i %l %u %t "%r" %s %b %{hashedClientId}s %{hashedRequestId}r %I %D"

Restart the service with the following command:

vmon-cli --restart vsphere-ui

Additional Information:

CCI-000067 Employ automated mechanisms to monitor remote access methods.

- NIST SP 800-53::AC-17 (1)
- NIST SP 800-53A::AC-17 (1).1
- NIST SP 800-53 Revision 4::AC-17 (1)
- NIST SP 800-53 Revision 5::AC-17 (1)

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-000166 Provide irrefutable evidence that an individual (or process acting on behalf of an individual) falsely denying having performed organization-defined actions to be covered by non-repudiation.

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

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-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-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-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

CCI-002234 Log the execution of privileged functions.

- NIST SP 800-53 Revision 4::AC-6 (9)
- NIST SP 800-53 Revision 5::AC-6 (9)

1.5 VCUI-80-000025 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter UI service must protect logs from unauthorized access.

```
GROUP ID: V-259108
RULE ID: SV-259108r960930
```

Rationale:

Log data is essential in the investigation of events. The accuracy of the information is always pertinent. One of the first steps an attacker will take is the modification or deletion of log records to cover tracks and prolong discovery. The web server must protect the log data from unauthorized modification.

Satisfies: SRG-APP-000118-AS-000078, SRG-APP-000119-AS-000079, SRG-APP-000120-AS-000080

Audit:

At the command prompt, run the following command:

find /var/log/vmware/vsphere-ui/ -xdev -type f -a '(' -perm -o+w -o -not -user vsphere-ui -o -not -group users -a -not -group root ')' -exec ls -ld {} ;

If any files are returned, this is a finding.

Remediation:

At the command prompt, run the following commands:

chmod o-w chown vsphere-ui:users

Note: Substitute with the listed file.

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

1.6 VCUI-80-000034 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter UI service must limit privileges for creating or modifying hosted application shared files.

```
GROUP ID: V-259109
RULE ID: SV-259109r960960
```

Rationale:

Application servers have the ability to specify that the hosted applications use shared libraries. The application server must have a capability to divide roles based upon duties wherein one project user (such as a developer) cannot modify the shared library code of another project user. The application server must also be able to specify that nonprivileged users cannot modify any shared library code at all.

Ensuring the Security Lifecycle Listener element is uncommented and sets a minimum Umask value will allow the server to perform a number of security checks when starting and prevent the service from starting if they fail.

Audit:

At the command prompt, run the following command:

xmllint --xpath
'/Server/Listener[@className="org.apache.catalina.security.SecurityListener"]'
/usr/lib/vmware-vsphere-ui/server/conf/server.xml

Example result:

If the "org.apache.catalina.security.SecurityListener" listener is not present, this is a finding.

If the "org.apache.catalina.security.SecurityListener" listener is configured with a "minimumUmask" and is not "0007", this is a finding.

Remediation:

Navigate to and open:

/usr/lib/vmware-vsphere-ui/server/conf/server.xml

Navigate to the <Server> node and add or update the "org.apache.catalina.security.SecurityListener" as follows:

Restart the service with the following command:

vmon-cli --restart vsphere-ui

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

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

1.7 VCUI-80-000036 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter UI service must disable stack tracing.

```
GROUP ID: V-259110
RULE ID: SV-259110r960963
```

Rationale:

Stack tracing provides debugging information from the application call stacks when a runtime error is encountered. If stack tracing is left enabled, Tomcat will provide this call stack information to the requestor, which could result in the loss of sensitive information or data that could be used to compromise the system.

Audit:

At the command prompt, run the following command:

xmllint --xpath "//Connector[@allowTrace = 'true']" /usr/lib/vmware-vsphere-ui/server/conf/server.xml

Expected result:

XPath set is empty

If any connectors are returned, this is a finding.

Remediation:

Navigate to and open:

/usr/lib/vmware-vsphere-ui/server/conf/server.xml

Navigate to and locate:

'allowTrace="true"'

Remove the 'allowTrace="true"' setting.

Note: If "allowTrace" is not present, it defaults to false.

Restart the service with the following command:

vmon-cli --restart vsphere-ui

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

1.8 VCUI-80-000037 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter UI service must be configured to use a specified IP address and port.

```
GROUP ID: V-259111
RULE ID: SV-259111r960966
```

Rationale:

The server must be configured to listen on a specified IP address and port. Without specifying an IP address and port for server to use, the server will listen on all IP addresses available.

Accessing the hosted application through an IP address normally used for nonapplication functions opens the possibility of user access to resources, utilities, files, ports, and protocols that are protected on the desired application IP address.

Audit:

At the command prompt, run the following command:

xmllint --xpath "//Connector[(@port = '0') or not(@address)]" /usr/lib/vmware-vsphere-ui/server/conf/server.xml

Expected result:

XPath set is empty

If any connectors are returned, this is a finding.

Remediation:

Navigate to and open:

/usr/lib/vmware-vsphere-ui/server/conf/server.xml

Navigate to the <Connector> node and configure the port and address as follows.

port="${http.port}" address="localhost"

Restart the service with the following command:

vmon-cli --restart vsphere-ui

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

1.9 VCUI-80-000057 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter UI service must be configured to limit data exposure between applications.

```
GROUP ID: V-259112
RULE ID: SV-259112r961116
```

Rationale:

If RECYCLE_FACADES is true or if a security manager is in use, a new facade object will be created for each request. This reduces the chances that a bug in an application might expose data from one request to another.

Audit:

At the command line, run the following command:

grep RECYCLE_FACADES /usr/lib/vmware-vsphere-ui/server/conf/catalina.properties

Example result:

org.apache.catalina.connector.RECYCLE_FACADES=true

If "org.apache.catalina.connector.RECYCLE_FACADES" is not set to "true", this is a finding.

If the "org.apache.catalina.connector.RECYCLE_FACADES" setting does not exist, this is not a finding.

Remediation:

Navigate to and open:

/usr/lib/vmware-vsphere-ui/server/conf/catalina.properties

Update or remove the following line:

org.apache.catalina.connector.RECYCLE_FACADES=true

Restart the service with the following command:

vmon-cli --restart vsphere-ui

Additional Information:

CCI-001664 Recognize only session identifiers that are system-generated.

- NIST SP 800-53::SC-23 (3)

- NIST SP 800-53A::SC-23 (3).1 (ii)
- NIST SP 800-53 Revision 4::SC-23 (3)
- NIST SP 800-53 Revision 5::SC-23 (3)

1.10 VCUI-80-000065 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter UI service must set URIEncoding to UTF-8.

```
GROUP ID: V-259114
RULE ID: SV-259114r961158
```

Rationale:

Invalid user input occurs when a user inserts data or characters into a hosted application's data entry field and the hosted application is unprepared to process that data. This results in unanticipated application behavior, potentially leading to an application compromise. Invalid user input is one of the primary methods employed when attempting to compromise an application.

An attacker can also enter Unicode characters into hosted applications in an effort to break out of the document home or root home directory or bypass security checks.

Audit:

At the command prompt, run the following command:

xmllint --xpath "//Connector[@URIEncoding != 'UTF-8'] | //Connector[not[@URIEncoding]]" /usr/lib/vmware-vsphere-ui/server/conf/server.xml

Expected result:

XPath set is empty

If any connectors are returned, this is a finding.

Remediation:

Navigate to and open:

/usr/lib/vmware-vsphere-ui/server/conf/server.xml

Configure the <Connector> node with the value:

URIEncoding="UTF-8"

Restart the service with the following command:

vmon-cli --restart vsphere-ui

Additional Information:

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

1.11 VCUI-80-000062 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter UI service must be configured to fail to a known safe state if system initialization fails.

```
GROUP ID: V-259113
RULE ID: SV-259113r961122
```

Rationale:

Determining a safe state for failure and weighing that against a potential denial of service for users depends on what type of application the web server is hosting. It is preferable that the service abort startup on any initialization failure rather than continuing in a degraded, and potentially insecure, state.

Audit:

At the command line, run the following command:

grep EXIT_ON_INIT_FAILURE /usr/lib/vmware-vsphere-ui/server/conf/catalina.properties

Example result:

org.apache.catalina.startup.EXIT_ON_INIT_FAILURE=true

If there are no results, or if the "org.apache.catalina.startup.EXIT_ON_INIT_FAILURE" is not set to "true", this is a finding.

Remediation:

Navigate to and open:

/usr/lib/vmware-vsphere-ui/server/conf/catalina.properties

Add or change the following line:

org.apache.catalina.startup.EXIT_ON_INIT_FAILURE=true

Restart the service with the following command:

vmon-cli --restart vsphere-ui

Additional Information:

CCI-001190 Fail to an organization-defined known-system state for the list of organization-defined types of system failures on organization-defined system components on the indicated components while preserving organization-defined system state information in failure.

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

1.12 VCUI-80-000067 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter UI service "ErrorReportValve showServerInfo" must be set to "false".

```
GROUP ID: V-259115
RULE ID: SV-259115r961167
```

Rationale:

The Error Report Valve is a simple error handler for HTTP status codes that will generate and return HTML error pages. It can also be configured to return predefined static HTML pages for specific status codes and/or exception types. Disabling "showServerInfo" will only return the HTTP status code and remove all CSS from the default nonerror-related HTTP responses.

Audit:

At the command prompt, run the following command:

xmllint --xpath '/Server/Service/Engine/Host/Valve[@className="org.apache.catalina.valves.ErrorReportValve"]' /usr/lib/vmware-vsphere-ui/server/conf/server.xml

Example result:

If the "ErrorReportValve" element is not defined or "showServerInfo" is not set to "false", this is a finding.

Remediation:

Navigate to and open:

/usr/lib/vmware-vsphere-ui/server/conf/server.xml

Locate the following Host block:

<Host ...> ... </Host>

Inside this block, add or update the following on a new line:

Restart the service with the following command:

vmon-cli --restart vsphere-ui

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

1.13 VCUI-80-000070 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter UI service must set an inactive timeout for sessions.

```
GROUP ID: V-259116
RULE ID: SV-259116r1003678
```

Rationale:

Leaving sessions open indefinitely is a major security risk. An attacker can easily use an already authenticated session to access the hosted application as the previously authenticated user. By closing sessions after a set period of inactivity, the web server can make certain that those sessions that are not closed through the user logging out of an application are eventually closed.

Satisfies: SRG-APP-000295-AS-000263, SRG-APP-000389-AS-000253

Audit:

At the command prompt, run the following command:

xmllint --format /usr/lib/vmware-vsphere-ui/server/conf/web.xml | sed 's/xmlns=".*"//g' | xmllint --xpath '/web-app/session-config/session-timeout' -

Example result:

30

If the value of "session-timeout" is not "30" or less, or is missing, this is a finding.

Remediation:

Navigate to and open:

/usr/lib/vmware-vsphere-ui/server/conf/web.xml

Navigate to the node and configure the as follows:

Restart the service with the following command:

vmon-cli --restart vsphere-ui

Additional Information:

CCI-004895 Permit users to invoke the trusted communications path for communications between the user and the organization-defined security functions, including at a minimum, authentication and re-authentication.

- NIST SP 800-53 Revision 5::SC-11 b

CCI-002361 Automatically terminate a user session after organization-defined conditions or trigger events requiring session disconnect.

- NIST SP 800-53 Revision 4::AC-12
- NIST SP 800-53 Revision 5::AC-12

1.14 VCUI-80-000081 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter UI service must offload log records onto a different system or media from the system being logged.

```
GROUP ID: V-259117
RULE ID: SV-259117r961395
```

Rationale:

Information system logging capability is critical for accurate forensic analysis. Log record content that may be necessary to satisfy the requirement of this control includes, but is not limited to, time stamps, source and destination IP addresses, user/process identifiers, event descriptions, application-specific events, success/fail indications, filenames involved, and access control or flow control rules invoked.

Offloading is a common process in information systems with limited log storage capacity.

Centralized management of log records provides for efficiency in maintenance and management of records, as well as the backup and archiving of those records. Application servers and their related components are required to offload log records onto a different system or media than the system being logged.

Audit:

By default, a vmware-services-vsphere-ui.conf rsyslog 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-vsphere-ui.conf

Expected result:

vsphere-ui main log input(type="imfile" File="/var/log/vmware/vsphere-ui/logs/vsphere_client_virgo.log" Tag="ui-main" Severity="info" Facility="local0") vsphere-ui change log input(type="imfile" File="/var/log/vmware/vsphere-ui/logs/changelog.log" Tag="ui-changelog" Severity="info" Facility="local0") vsphere-ui dataservice log input(type="imfile" File="/var/log/vmware/vsphere-ui/logs/dataservice.log" Tag="ui-dataservice" Severity="info" Facility="local0") vsphere-ui apigw log input(type="imfile" File="/var/log/vmware/vsphere-ui/logs/apigw.log" Tag="ui-apigw" Severity="info" Facility="local0") vsphere-ui equinox log input(type="imfile" File="/var/log/vmware/vsphere-ui/logs/equinox.log" Tag="ui-equinox" Severity="info" Facility="local0") vsphere-ui event log input(type="imfile" File="/var/log/vmware/vsphere-ui/logs/eventlog.log" Tag="ui-eventlog" Severity="info" Facility="local0") vsphere-ui op id log input(type="imfile" File="/var/log/vmware/vsphere-ui/logs/opId.log" Tag="ui-opid" Severity="info" Facility="local0") vsphere-ui performance audit log input(type="imfile" File="/var/log/vmware/vsphere-ui/logs/performanceAudit.log" Tag="ui-performanceAudit" Severity="info" Facility="local0") vsphere-ui plugin-medic log input(type="imfile" File="/var/log/vmware/vsphere-ui/logs/plugin-medic.log" Tag="ui-plugin-medic" Severity="info" Facility="local0") vsphere-ui threadmonitor log input(type="imfile" File="/var/log/vmware/vsphere-ui/logs/threadmonitor.log" Tag="ui-threadmonitor" Severity="info" Facility="local0") vsphere-ui threadpools log input(type="imfile" File="/var/log/vmware/vsphere-ui/logs/threadpools.log" Tag="ui-threadpools" Severity="info" Facility="local0") vsphere-ui vspheremessaging log input(type="imfile" File="/var/log/vmware/vsphere-ui/logs/vspheremessaging.log" Tag="ui-vspheremessaging" Severity="info" Facility="local0") vsphere-ui rpm log input(type="imfile" File="/var/log/vmware/vsphere-ui/logs/vsphere-ui-rpm.log" Tag="ui-rpm" Severity="info" Facility="local0") vsphere-ui runtime log stdout input(type="imfile" File="/var/log/vmware/vsphere-ui/logs/vsphere-ui-runtime.log*" Tag="ui-runtime-stdout" Severity="info" Facility="local0") vsphere-ui runtime log stderr input(type="imfile" File="/var/log/vmware/vsphere-ui/logs/vsphere-ui-runtime.log*" Tag="ui-runtime-stderr" Severity="info" Facility="local0") vsphere-ui access log input(type="imfile" File="/var/log/vmware/vsphere-ui/logs/access/localhost_access_log.txt" Tag="ui-access" Severity="info" Facility="local0") vsphere-ui gc log input(type="imfile" File="/var/log/vmware/vsphere-ui/vsphere-ui-gc*" Tag="ui-gc" Severity="info" Facility="local0") vsphere-ui firstboot log input(type="imfile" File="/var/log/firstboot/vsphere_ui_firstboot*" Tag="ui-firstboot" Severity="info" Facility="local0") vsphere-ui catalina input(type="imfile" File="/var/log/vmware/vsphere-ui/logs/catalina.*.log" Tag="ui-runtime-catalina" Severity="info" Facility="local0") vsphere-ui endpoint input(type="imfile" File="/var/log/vmware/vsphere-ui/logs/endpoint.log" Tag="ui-runtime-endpoint" Severity="info" Facility="local0") vsphere-ui localhost input(type="imfile" File="/var/log/vmware/vsphere-ui/logs/localhost.*.log" Tag="ui-runtime-localhost" Severity="info" Facility="local0") vsphere-ui vsan input(type="imfile" File="/var/log/vmware/vsphere-ui/logs/vsan-plugin.log" Tag="ui-runtime-vsan" Severity="info" Facility="local0")

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

Remediation:

Navigate to and open:

vmware-services-vsphere-ui.conf

Create the file if it does not exist.

Set the contents of the file as follows:

vsphere-ui main log input(type="imfile" File="/var/log/vmware/vsphere-ui/logs/vsphere_client_virgo.log" Tag="ui-main" Severity="info" Facility="local0") vsphere-ui change log input(type="imfile" File="/var/log/vmware/vsphere-ui/logs/changelog.log" Tag="ui-changelog" Severity="info" Facility="local0") vsphere-ui dataservice log input(type="imfile" File="/var/log/vmware/vsphere-ui/logs/dataservice.log" Tag="ui-dataservice" Severity="info" Facility="local0") vsphere-ui apigw log input(type="imfile" File="/var/log/vmware/vsphere-ui/logs/apigw.log" Tag="ui-apigw" Severity="info" Facility="local0") vsphere-ui equinox log input(type="imfile" File="/var/log/vmware/vsphere-ui/logs/equinox.log" Tag="ui-equinox" Severity="info" Facility="local0") vsphere-ui event log input(type="imfile" File="/var/log/vmware/vsphere-ui/logs/eventlog.log" Tag="ui-eventlog" Severity="info" Facility="local0") vsphere-ui op id log input(type="imfile" File="/var/log/vmware/vsphere-ui/logs/opId.log" Tag="ui-opid" Severity="info" Facility="local0") vsphere-ui performance audit log input(type="imfile" File="/var/log/vmware/vsphere-ui/logs/performanceAudit.log" Tag="ui-performanceAudit" Severity="info" Facility="local0") vsphere-ui plugin-medic log input(type="imfile" File="/var/log/vmware/vsphere-ui/logs/plugin-medic.log" Tag="ui-plugin-medic" Severity="info" Facility="local0") vsphere-ui threadmonitor log input(type="imfile" File="/var/log/vmware/vsphere-ui/logs/threadmonitor.log" Tag="ui-threadmonitor" Severity="info" Facility="local0") vsphere-ui threadpools log input(type="imfile" File="/var/log/vmware/vsphere-ui/logs/threadpools.log" Tag="ui-threadpools" Severity="info" Facility="local0") vsphere-ui vspheremessaging log input(type="imfile" File="/var/log/vmware/vsphere-ui/logs/vspheremessaging.log" Tag="ui-vspheremessaging" Severity="info" Facility="local0") vsphere-ui rpm log input(type="imfile" File="/var/log/vmware/vsphere-ui/logs/vsphere-ui-rpm.log" Tag="ui-rpm" Severity="info" Facility="local0") vsphere-ui runtime log stdout input(type="imfile" File="/var/log/vmware/vsphere-ui/logs/vsphere-ui-runtime.log*" Tag="ui-runtime-stdout" Severity="info" Facility="local0") vsphere-ui runtime log stderr input(type="imfile" File="/var/log/vmware/vsphere-ui/logs/vsphere-ui-runtime.log*" Tag="ui-runtime-stderr" Severity="info" Facility="local0") vsphere-ui access log input(type="imfile" File="/var/log/vmware/vsphere-ui/logs/access/localhost_access_log.txt" Tag="ui-access" Severity="info" Facility="local0") vsphere-ui gc log input(type="imfile" File="/var/log/vmware/vsphere-ui/vsphere-ui-gc*" Tag="ui-gc" Severity="info" Facility="local0") vsphere-ui firstboot log input(type="imfile" File="/var/log/firstboot/vsphere_ui_firstboot*" Tag="ui-firstboot" Severity="info" Facility="local0") vsphere-ui catalina input(type="imfile" File="/var/log/vmware/vsphere-ui/logs/catalina.*.log" Tag="ui-runtime-catalina" Severity="info" Facility="local0") vsphere-ui endpoint input(type="imfile" File="/var/log/vmware/vsphere-ui/logs/endpoint.log" Tag="ui-runtime-endpoint" Severity="info" Facility="local0") vsphere-ui localhost input(type="imfile" File="/var/log/vmware/vsphere-ui/logs/localhost.*.log" Tag="ui-runtime-localhost" Severity="info" Facility="local0") vsphere-ui vsan input(type="imfile" File="/var/log/vmware/vsphere-ui/logs/vsan-plugin.log" Tag="ui-runtime-vsan" 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)

1.15 VCUI-80-000124 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter UI service must enable "STRICT_SERVLET_COMPLIANCE".

```
GROUP ID: V-259118
RULE ID: SV-259118r961863
```

Rationale:

Strict Servlet Compliance forces Tomcat to adhere to standards specifications including but not limited to RFC2109. RFC2109 sets the standard for HTTP session management. This setting affects several other settings that primarily pertain to cookie headers, cookie values, and sessions. Cookies will be parsed for strict adherence to specifications.

Note that changing a number of these default settings may break some systems, as some browsers are unable to correctly handle the cookie headers that result from a strict adherence to the specifications.

This one setting changes the default values for the following settings:

org.apache.catalina.core.ApplicationContext.GET_RESOURCE_REQUIRE_SLASH
org.apache.catalina.core.ApplicationDispatcher.WRAP_SAME_OBJECT
org.apache.catalina.core.StandardHostValve.ACCESS_SESSION
org.apache.catalina.session.StandardSession.ACTIVITY_CHECK
org.apache.catalina.session.StandardSession.LAST_ACCESS_AT_START
org.apache.tomcat.util.http.ServerCookie.ALWAYS_ADD_EXPIRES
org.apache.tomcat.util.http.ServerCookie.FWD_SLASH_IS_SEPARATOR
org.apache.tomcat.util.http.ServerCookie.PRESERVE_COOKIE_HEADER
org.apache.tomcat.util.http.ServerCookie.STRICT_NAMING The "resourceOnlyServlets" attribute of any Context element. The "tldValidation" attribute of any Context element. The "useRelativeRedirects" attribute of any Context element. The "xmlNamespaceAware" attribute of any Context element. The "xmlValidation" attribute of any Context element.

Audit:

At the command line, run the following command:

grep STRICT_SERVLET_COMPLIANCE /usr/lib/vmware-vsphere-ui/server/conf/catalina.properties

Example result:

org.apache.catalina.STRICT_SERVLET_COMPLIANCE=true

If there are no results, or if the "org.apache.catalina.STRICT_SERVLET_COMPLIANCE" is not set to "true", this is a finding.

Remediation:

Navigate to and open:

/usr/lib/vmware-vsphere-ui/server/conf/catalina.properties

Add or change the following line:

org.apache.catalina.STRICT_SERVLET_COMPLIANCE=true

Restart the service with the following command:

vmon-cli --restart vsphere-ui

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

1.16 VCUI-80-000125 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter UI service must limit the amount of time that each Transmission Control Protocol (TCP) connection is kept alive.

```
GROUP ID: V-259119
RULE ID: SV-259119r960735
```

Rationale:

Denial of service (DoS) is one threat against web servers. Many DoS attacks attempt to consume web server resources in such a way that no more resources are available to satisfy legitimate requests.

In Tomcat, the "connectionTimeout" attribute sets the number of milliseconds the server will wait after accepting a connection for the request Uniform Resource Identifier (URI) line to be presented. This timeout will also be used when reading the request body (if any). This prevents idle sockets that are not sending HTTP requests from consuming system resources and potentially denying new connections.

Audit:

The connection timeout should not be disabled by setting it to "-1".

At the command prompt, run the following command:

xmllint --xpath "//Connector[@connectionTimeout = '-1']" /usr/lib/vmware-vsphere-ui/server/conf/server.xml

Expected result:

XPath set is empty

If any connectors are returned, this is a finding.

Remediation:

Navigate to and open:

/usr/lib/vmware-vsphere-ui/server/conf/server.xml

Configure the <Connector> node with the value:

connectionTimeout="300000"

Restart the service with the following command:

vmon-cli --restart vsphere-ui

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

1.17 VCUI-80-000126 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter UI service must limit the number of times that each Transmission Control Protocol (TCP) connection is kept alive.

```
GROUP ID: V-259120
RULE ID: SV-259120r960735
```

Rationale:

KeepAlive provides long lived HTTP sessions that allow multiple requests to be sent over the same connection. Enabling KeepAlive mitigates the effects of several types of denial-of-service attacks.

An advantage of KeepAlive is the reduced latency in subsequent requests (no handshaking). However, a disadvantage is that server resources are not available to handle other requests while a connection is maintained between the server and the client.

Tomcat can be configured to limit the number of subsequent requests that one client can submit to the server over an established connection. This limit helps provide a balance between the advantages of KeepAlive, while not allowing any one connection being held too long by any one client.

Audit:

The connection timeout should not be unlimited by setting it to "-1".

At the command prompt, run the following command:

xmllint --xpath "//Connector[@maxKeepAliveRequests = '-1']" /usr/lib/vmware-vsphere-ui/server/conf/server.xml

Expected result:

XPath set is empty

If any connectors are returned, this is a finding.

Remediation:

Navigate to and open:

/usr/lib/vmware-vsphere-ui/server/conf/server.xml

Configure the <Connector> node with the value:

maxKeepAliveRequests="100"

Restart the service with the following command:

vmon-cli --restart vsphere-ui

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

1.18 VCUI-80-000127 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter UI service must configure the "setCharacterEncodingFilter" filter.

```
GROUP ID: V-259121
RULE ID: SV-259121r961158
```

Rationale:

Invalid user input occurs when a user inserts data or characters into a hosted application's data entry field and the hosted application is unprepared to process that data. This results in unanticipated application behavior, potentially leading to an application compromise. Invalid user input is one of the primary methods employed when attempting to compromise an application.

An attacker can also enter Unicode characters into hosted applications in an effort to break out of the document home or root home directory or to bypass security checks. VMware uses the standard Tomcat "SetCharacterEncodingFilter" to provide a layer of defense against character encoding attacks. Filters are Java objects that perform filtering tasks on the request to a resource (a servlet or static content), on the response from a resource, or both.

Audit:

At the command prompt, run the following command:

xmllint --xpath "//*[contains(text(), 'setCharacterEncodingFilter')]/parent::*" /usr/lib/vmware-vsphere-ui/server/conf/web.xml

Expected result:

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

Remediation:

Navigate to and open:

/usr/lib/vmware-vsphere-ui/server/conf/web.xml

Configure the node with the child nodes listed below:

Restart the service with the following command:

vmon-cli --restart vsphere-ui

Additional Information:

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

1.19 VCUI-80-000129 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter UI service cookies must have "http-only" flag set.

```
GROUP ID: V-259122
RULE ID: SV-259122r960792
```

Rationale:

Cookies are a common way to save session state over the HTTP(S) protocol. If attackers can compromise session data stored in a cookie, they are better able to launch an attack against the server and its applications. When a cookie is tagged with the "HttpOnly" flag, it tells the browser this particular cookie should only be accessed by the originating server. Any attempt to access the cookie from client script is strictly forbidden.

Audit:

At the command prompt, run the following command:

xmllint --format /usr/lib/vmware-vsphere-ui/server/conf/web.xml | sed 's/xmlns=".*"//g' | xmllint --xpath '/web-app/session-config/cookie-config/http-only' -

Expected result:

true

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

Remediation:

Navigate to and open:

/usr/lib/vmware-vsphere-ui/server/conf/web.xml

Navigate to the node and configure the as follows:

Restart the service with the following command:

vmon-cli --restart vsphere-ui

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3

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

1.20 VCUI-80-000130 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter UI service DefaultServlet must be set to "readonly" for "PUT" and "DELETE" commands.

```
GROUP ID: V-259123
RULE ID: SV-259123r960792
```

Rationale:

The default servlet (or DefaultServlet) is a special servlet provided with Tomcat that is called when no other suitable page is found in a particular folder. The DefaultServlet serves static resources as well as directory listings. The DefaultServlet is configured by default with the "readonly" parameter set to "true" where HTTP commands such as "PUT" and "DELETE" are rejected.

Changing this to "false" allows clients to delete or modify static resources on the server and to upload new resources. DefaultServlet "readonly" must be set to "true", either literally or by absence (default).

Audit:

At the command prompt, run the following command:

xmllint --xpath "//*[contains(text(), 'DefaultServlet')]/parent::*" /usr/lib/vmware-vsphere-ui/server/conf/web.xml

Example output:

If the "readOnly" param-value for the "DefaultServlet" servlet class is set to "false", this is a finding.

If the "readOnly" param-value does not exist, this is not a finding.

Remediation:

Navigate to and open:

/usr/lib/vmware-vsphere-ui/server/conf/web.xml

Navigate to the ///org.apache.catalina.servlets.DefaultServlet/ node and remove the following node:

Restart the service with the following command:

vmon-cli --restart vsphere-ui

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

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

1.21 VCUI-80-000134 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter UI service shutdown port must be disabled.

```
GROUP ID: V-259124
RULE ID: SV-259124r960963
```

Rationale:

Tomcat by default listens on TCP port 8005 to accept shutdown requests. By connecting to this port and sending the SHUTDOWN command, all applications within Tomcat are halted. The shutdown port is not exposed to the network as it is bound to the loopback interface. Setting the port to "-1" in $CATALINA_BASE/conf/server.xml instructs Tomcat to not listen for the shutdown command.

Audit:

At the command prompt, run the following commands:

xmllint --xpath "//Server/@port" /usr/lib/vmware-vsphere-ui/server/conf/server.xml grep shutdown.port /etc/vmware/vmware-vmon/svcCfgfiles/vsphere-ui.json

Example results:

port="${shutdown.port}" "-Dshutdown.port=-1",

If "port" does not equal "${shutdown.port}", this is a finding.

If "shutdown.port" does not equal "-1", this is a finding.

Remediation:

Navigate to and open:

/usr/lib/vmware-vsphere-ui/server/conf/catalina.properties

Add or modify the setting "shutdown.port=-1" in the "catalina.properties" file.

Navigate to and open:

/usr/lib/vmware-vsphere-ui/server/conf/server.xml

Configure the <Server> node with the value:

port="${shutdown.port}"

Restart the service with the following command:

vmon-cli --restart vsphere-ui

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

1.22 VCUI-80-000137 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter UI service directory listings parameter must be disabled.

```
GROUP ID: V-259126
RULE ID: SV-259126r960963
```

Rationale:

Enumeration techniques, such as URL parameter manipulation, rely on being able to obtain information about the web server's directory structure by locating directories without default pages. In this scenario, the web server will display to the user a listing of the files in the directory being accessed. Ensuring that directory listing is disabled is one approach to mitigating the vulnerability.

In Tomcat, directory listing is disabled by default but can be enabled via the "listings" parameter. Ensure this node is not present to have the default effect.

Audit:

At the command prompt, run the following command:

xmllint --format /usr/lib/vmware-vsphere-ui/server/conf/web.xml | sed 's/xmlns=".*"//g' | xmllint --xpath '//param-name[text()="listings"]/parent::init-param' -

Example result:

XPath set is empty

If the "listings" parameter is specified and is not "false", this is a finding.

If the "listings" parameter does not exist, this is not a finding.

Remediation:

Navigate to and open:

/usr/lib/vmware-vsphere-ui/server/conf/web.xml

Find and remove the entire block returned in the check.

Example:

Restart the service with the following command:

vmon-cli --restart vsphere-ui

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

1.23 VCUI-80-000136 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter UI service debug parameter must be disabled.

```
GROUP ID: V-259125
RULE ID: SV-259125r960963
```

Rationale:

Information needed by an attacker to begin looking for possible vulnerabilities in a web server includes any information about the web server and plug-ins or modules being used. When debugging or trace information is enabled in a production web server, information about the web server, such as web server type, version, patches installed, plug-ins and modules installed, type of code being used by the hosted application, and any backends being used for data storage may be displayed.

Because this information may be placed in logs and general messages during normal operation of the web server, an attacker does not need to cause an error condition to gain this information.

Audit:

At the command prompt, run the following command:

xmllint --format /usr/lib/vmware-vsphere-ui/server/conf/web.xml | sed 's/xmlns=".*"//g' | xmllint --xpath '//param-name[text()="debug"]/parent::init-param' -

Example result:

If the "debug" parameter is specified and is not "0", this is a finding.

If the "debug" parameter does not exist, this is not a finding.

Remediation:

Navigate to and open:

/usr/lib/vmware-vsphere-ui/server/conf/web.xml

Navigate to all nodes that are not set to "0".

Set the to "0" in all debug nodes.

Note: The debug setting should look like the following:

Restart the service with the following command:

vmon-cli --restart vsphere-ui

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

1.24 VCUI-80-000138 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter UI service deployXML attribute must be disabled.

```
GROUP ID: V-259127
RULE ID: SV-259127r960963
```

Rationale:

The Host element controls deployment. Automatic deployment allows for simpler management but also makes it easier for an attacker to deploy a malicious application. Automatic deployment is controlled by the autoDeploy and deployOnStartup attributes. If both are false, only Contexts defined in server.xml will be deployed, and any changes will require a Tomcat restart.

In a hosted environment where web applications may not be trusted, set the deployXML attribute to "false" to ignore any context.xml packaged with the web application that may try to assign increased privileges to the web application. Note that if the security manager is enabled, the deployXML attribute will default to false.

Audit:

At the command prompt, run the following command:

xmllint --xpath "//Host/@deployXML" /usr/lib/vmware-vsphere-ui/server/conf/server.xml

Expected result:

deployXML="false"

If "deployXML" does not equal "false", this is a finding.

Remediation:

Navigate to and open:

/usr/lib/vmware-vsphere-ui/server/conf/server.xml

Navigate to the <Host> node and configure with the value "deployXML="false"".

Restart the service with the following command:

vmon-cli --restart vsphere-ui

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

1.25 VCUI-80-000139 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter UI service must have Autodeploy disabled.

```
GROUP ID: V-259128
RULE ID: SV-259128r960963
```

Rationale:

Tomcat allows auto-deployment of applications while it is running. This can allow untested or malicious applications to be automatically loaded into production. Autodeploy must be disabled in production.

Audit:

At the command prompt, run the following command:

xmllint --xpath "//Host/@autoDeploy" /usr/lib/vmware-vsphere-ui/server/conf/server.xml

Expected result:

autoDeploy="false"

If "autoDeploy" does not equal "false", this is a finding.

Remediation:

Navigate to and open:

/usr/lib/vmware-vsphere-ui/server/conf/server.xml

Navigate to the <Host> node and configure with the value "autoDeploy="false"".

Restart the service with the following command:

vmon-cli --restart vsphere-ui

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

1.26 VCUI-80-000140 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter UI service xpoweredBy attribute must be disabled.

```
GROUP ID: V-259129
RULE ID: SV-259129r960963
```

Rationale:

Individual connectors can be configured to display the Tomcat information to clients. This information can be used to identify server versions that can be useful to attackers for identifying vulnerable versions of Tomcat. Individual connectors must be checked for the xpoweredBy attribute to ensure they do not pass server information to clients. The default value for xpoweredBy is "false".

Audit:

At the command prompt, run the following command:

xmllint --xpath "//Connector/@xpoweredBy" /usr/lib/vmware-vsphere-ui/server/conf/server.xml

Example result:

XPath set is empty

If the "xpoweredBy" parameter is specified and is not "false", this is a finding.

If the "xpoweredBy" parameter does not exist, this is not a finding.

Remediation:

Navigate to and open:

/usr/lib/vmware-vsphere-ui/server/conf/server.xml

Navigate to the <Connector> node and remove the "xpoweredBy" attribute.

Restart the service with the following command:

vmon-cli --restart vsphere-ui

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

1.27 VCUI-80-000141 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter UI service example applications must be removed.

```
GROUP ID: V-259130
RULE ID: SV-259130r960963
```

Rationale:

Tomcat provides example applications, documentation, and other directories in the default installation that do not serve a production use. These files must be deleted.

Audit:

At the command prompt, run the following command:

ls -l /usr/lib/vmware-vsphere-ui/server/webapps/examples

If the examples folder exists or contains any content, this is a finding.

Remediation:

At the command prompt, run the following command:

rm -rf /usr/lib/vmware-vsphere-ui/server/webapps/examples

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

1.28 VCUI-80-000142 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter UI service default ROOT web application must be removed.

```
GROUP ID: V-259131
RULE ID: SV-259131r960963
```

Rationale:

The default ROOT web application includes the version of Tomcat being used, links to Tomcat documentation, examples, FAQs, and mailing lists. The default ROOT web application must be removed from a publicly accessible instance and a more appropriate default page shown to users.

Audit:

At the command prompt, run the following command:

ls -l /usr/lib/vmware-vsphere-ui/server/webapps/ROOT

If the ROOT web application contains any content, this is a finding.

Remediation:

At the command prompt, run the following command:

rm -rf /usr/lib/vmware-vsphere-ui/server/webapps/ROOT/*

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

1.29 VCUI-80-000143 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter UI service default documentation must be removed.

```
GROUP ID: V-259132
RULE ID: SV-259132r960963
```

Rationale:

Tomcat provides documentation and other directories in the default installation that do not serve a production use. These files must be deleted.

Audit:

At the command prompt, run the following command:

ls -l /usr/lib/vmware-vsphere-ui/server/webapps/docs

If the "docs" folder exists or contains any content, this is a finding.

Remediation:

At the command prompt, run the following command:

rm -rf /usr/lib/vmware-vsphere-ui/server/webapps/docs

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

1.30 VCUI-80-000151 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter UI service must disable "ALLOW_BACKSLASH".

```
GROUP ID: V-259133
RULE ID: SV-259133r961863
```

Rationale:

When Tomcat is installed behind a proxy configured to only allow access to certain contexts (web applications), an HTTP request containing "/../" may allow attackers to work around the proxy restrictions using directory traversal attack methods. If "allow_backslash" is "true", the "" character will be permitted as a path delimiter. The default value for the setting is "false", but Tomcat must always be configured as if no proxy restricting context access was used, and "allow_backslash" should be set to "false" to prevent directory-traversal-style attacks. This setting can create operability issues with noncompliant clients.

Audit:

At the command line, run the following command:

grep ALLOW_BACKSLASH /usr/lib/vmware-vsphere-ui/server/conf/catalina.properties

Example result:

org.apache.catalina.connector.ALLOW_BACKSLASH=false

If "org.apache.catalina.connector.ALLOW_BACKSLASH" is not set to "false", this is a finding.

If the "org.apache.catalina.connector.ALLOW_BACKSLASH" setting does not exist, this is not a finding.

Remediation:

Navigate to and open:

/usr/lib/vmware-vsphere-ui/server/conf/catalina.properties

Update or remove the following line:

org.apache.catalina.connector.ALLOW_BACKSLASH=false

Restart the service with the following command:

vmon-cli --restart vsphere-ui

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 VCUI-80-000152 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter UI service must enable "ENFORCE_ENCODING_IN_GET_WRITER".

```
GROUP ID: V-259134
RULE ID: SV-259134r961863
```

Rationale:

Some clients try to guess the character encoding of text media when the mandated default of ISO-8859-1 should be used. Some browsers will interpret as UTF-7 when the characters are safe for ISO-8859-1. This can create the potential for a XSS attack. To defend against this, enforce_encoding_in_get_writer must be set to true.

Audit:

At the command line, run the following command:

grep ENFORCE_ENCODING_IN_GET_WRITER /usr/lib/vmware-vsphere-ui/server/conf/catalina.properties

Example result:

org.apache.catalina.connector.response.ENFORCE_ENCODING_IN_GET_WRITER=true

If "org.apache.catalina.connector.response.ENFORCE_ENCODING_IN_GET_WRITER" is not set to "true", this is a finding.

If the "org.apache.catalina.connector.response.ENFORCE_ENCODING_IN_GET_WRITER" setting does not exist, this is not a finding.

Remediation:

Navigate to and open:

/usr/lib/vmware-vsphere-ui/server/conf/catalina.properties

Update or remove the following line:

org.apache.catalina.connector.response.ENFORCE_ENCODING_IN_GET_WRITER=true

Restart the service with the following command:

vmon-cli --restart vsphere-ui

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

1.32 VCUI-80-000154 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter UI service manager webapp must be removed.

```
GROUP ID: V-259135
RULE ID: SV-259135r960963
```

Rationale:

Tomcat provides management functionality through either a default manager webapp or through local editing of the configuration files. The manager webapp files must be deleted, and administration must be performed through the local editing of the configuration files.

Audit:

At the command prompt, run the following command:

ls -l /usr/lib/vmware-vsphere-ui/server/webapps/manager

If the manager folder exists or contains any content, this is a finding.

Remediation:

At the command prompt, run the following command:

rm -rf /usr/lib/vmware-vsphere-ui/server/webapps/manager

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

1.33 VCUI-80-000155 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter UI service host-manager webapp must be removed.

```
GROUP ID: V-259136
RULE ID: SV-259136r1003680
```

Rationale:

Tomcat provides host management functionality through either a default host-manager webapp or through local editing of the configuration files. The host-manager webapp files must be deleted, and administration must be performed through the local editing of the configuration files.

Audit:

At the command prompt, run the following command:

ls -l /usr/lib/vmware-vsphere-ui/server/webapps/host-manager

If the host-manager folder exists or contains any content, this is a finding.

Remediation:

At the command prompt, run the following command:

rm -rf /usr/lib/vmware-vsphere-ui/server/webapps/host-manager

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

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	VCUI-80-000001 (Manual)	☐	☐
1.2	VCUI-80-000005 (Manual)	☐	☐
1.3	VCUI-80-000013 (Manual)	☐	☐
1.4	VCUI-80-000014 (Manual)	☐	☐
1.5	VCUI-80-000025 (Manual)	☐	☐
1.6	VCUI-80-000034 (Manual)	☐	☐
1.7	VCUI-80-000036 (Manual)	☐	☐
1.8	VCUI-80-000037 (Manual)	☐	☐
1.9	VCUI-80-000057 (Manual)	☐	☐
1.10	VCUI-80-000065 (Manual)	☐	☐
1.11	VCUI-80-000062 (Manual)	☐	☐
1.12	VCUI-80-000067 (Manual)	☐	☐
1.13	VCUI-80-000070 (Manual)	☐	☐
1.14	VCUI-80-000081 (Manual)	☐	☐
1.15	VCUI-80-000124 (Manual)	☐	☐
1.16	VCUI-80-000125 (Manual)	☐	☐
1.17	VCUI-80-000126 (Manual)	☐	☐
1.18	VCUI-80-000127 (Manual)	☐	☐
1.19	VCUI-80-000129 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	VCUI-80-000130 (Manual)	☐	☐
1.21	VCUI-80-000134 (Manual)	☐	☐
1.22	VCUI-80-000137 (Manual)	☐	☐
1.23	VCUI-80-000136 (Manual)	☐	☐
1.24	VCUI-80-000138 (Manual)	☐	☐
1.25	VCUI-80-000139 (Manual)	☐	☐
1.26	VCUI-80-000140 (Manual)	☐	☐
1.27	VCUI-80-000141 (Manual)	☐	☐
1.28	VCUI-80-000142 (Manual)	☐	☐
1.29	VCUI-80-000143 (Manual)	☐	☐
1.30	VCUI-80-000151 (Manual)	☐	☐
1.31	VCUI-80-000152 (Manual)	☐	☐
1.32	VCUI-80-000154 (Manual)	☐	☐
1.33	VCUI-80-000155 (Manual)	☐	☐

Appendix: Change History

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