Nginx/HTTP - Web Security Features

For the Cisco IOS XE Everest 16.4.1 release, the following web security enhancements have been included:

- SSL/TLS Version for HTTP secure-server can be specified.
- Security headers enhancements

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Nginx/HTTP Web Security Features

- SSL/TLS Version for HTTP secure-server -- This enhancement is used to specify the TLS version to be used for HTTPS Server and HTTPS client sessions.
  - HTTPS Server command -- By default, it supports three versions. If you want to use a particular version for the sessions, you can specify by configuring the **ip http tls-version** command in global configuration mode. The versions are TLSv1.0, TLSv1.1, and TLSv1.2.
  - HTTPS Client command -- By default, it supports three versions. If you want to use a particular version for the sessions, you can specify by configuring the **ip http client tls-version** command in global configuration mode. The versions are TLSv1.0, TLSv1.1, and TLSv1.2.

Note These commands allow you to set the particular version used for sessions. The underlying SSL infrastructure supports the option of specifying either all or only one TLS version. Hence the HTTPS provides the option to specify the individual version. Use the **no** form of the command to remove the configuration.

- Security Header Enhancements
  - HTTP Server – The following headers are the web server security enhancements. The actual headers and respective values appear in the response by default:

    X-XSS-Protection: 1; mode=block -- This header indicates that XSS protection is enabled [value 1] and if the browser finds any attack, it should block rendering the page.

    X-Frame-Options: SAMEORIGIN - Allows the contents to be rendered in a frame if it belongs to the same domain.

    X-Content-Type-Options: nosniff - Prevents the browser from doing MIME-type sniffing.

    Strict-Transport-Security: max-age=7884000 - Strict-Transport-Security HTTP header. Use the [no] ip http HSTS-Header to enable/disable this header for IOS applications. By default, it is enabled and use the no ip http HSTS-Header command disable this header from the response.
  - Nginx – Web user interface - Nginx applications take care of the headers for their response. As Web UI is one of the NginX application, it adds the security headers. The three headers are the following:
    - X-XSS-Protection: 1; mode=block
    - X-Frame-Options: SAMEORIGIN
    - X-Content-Type-Options: nosniff

Verifying the Configured Version

Use the **show ip http client all** command to see the currently enabled TLS version.

```
Device# show ip http client all

<snip>

Maximum number of requests allowed on a connection: 25
Server linger time : 60 seconds
HTTP server active session modules: ALL
HTTP secure server capability: Present
HTTP secure server status: Enabled
HTTP secure server port: 443
HTTP secure server ciphersuite: 3des-ede-cbc-sha aes-128-cbc-sha
aes-256-cbc-sha dhe-aes-128-cbc-sha ecdhe-rsa-3des-ede-cbc-sha
HTTP secure server TLS version: TLSv1.2 TLSv1.1 TLSv1.0    <<<This line shows the TLS version
 that is enabled.
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint:
HTTP secure server active session modules: ALL

<snip>
```

Use the **show http server status** command to see the currently enabled TLS version.

```
Device# show http server status

<snip>
```

```
Maximum number of concurrent server connections allowed: 50
Maximum number of secondary server connections allowed: 50
Server idle time-out: 180 seconds
Server life time-out: 180 seconds
Server session idle time-out: 180 seconds
Maximum number of requests allowed on a connection: 25
Server linger time : 60 seconds
HTTP server active session modules: ALL
HTTP secure server capability: Present
HTTP secure server status: Enabled
HTTP secure server port: 443
HTTP secure server ciphersuite: 3des-ede-cbc-sha aes-128-cbc-sha
aes-256-cbc-sha dhe-aes-128-cbc-sha ecdhe-rsa-3des-ede-cbc-sha
HTTP secure server TLS version: TLSv1.2 TLSv1.1 TLSv1.0   <<<This line shows the TLS version
 that is enabled.
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint:

<snip>
```

Additional References

Related Documents

Related Topic	Document Title
Additional HTTP configuration information	*Using the Cisco Web Browser User Interface*
Additional HTTPS configuration information	*HTTPS - HTTP Server and Client with SSL 3.0*
Additional HTTP and HTTPS commands	*Cisco IOS Network Management Command Reference*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/public/support/tac/home.shtml

Feature Information for Nginx/HTTP -- Web Security Features

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Nginx/HTTP -- Web Security Features

Feature Name	Releases	Feature Information
Nginx/HTTP -- Web Security Features	Cisco IOS XE Everest 16.4.1 Release	For the Cisco IOS XE Everest 16.4.1 release, the following web security enhancements have been included: • SSL/TLS Version for HTTP secure-server can be specified. • Security headers enhancements