Release Notes for Catalyst 6500 Series SSL Services Module Software Release 1.x

Current Release: 1.2(2)—January 15, 2004

Previous release: 1.2(1), 1.1(1)

The SSL Services Module is a Layer 4 through Layer 7 service module that you can install into the Catalyst 6500 series switch. The module terminates secure sockets layer (SSL) transactions and accelerates the encryption and decryption of data used in SSL sessions.

This publication describes the features, modifications, and caveats for the Catalyst 6500 series SSL Services Module software release 1.*x*.

Note For detailed installation and configuration procedures for the SSL Services Module, refer to the *Catalyst 6500 Series SSL Services Module Installation and Configuration Note* at this URL:

http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/ssl/2.1/Install/78_15947.html

Contents

This document consists of these sections:

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

System Requirements

This section describes the system requirements for the Catalyst 6500 series SSL Services Module software release 1.x:

Memory Requirements

The Catalyst 6500 series SSL Services Module memory is not configurable.

Hardware Requirements

The Catalyst 6500 series SSL Services Module is supported in systems with Supervisor Engine 2 with an MSFC 2 or Supervisor Engine 720 with an MSFC3, and any module with ports that connect server and client networks.

Software Requirements

Table 1 lists the SSL software versions supported by Catalyst operating system and Cisco IOS software.

Table 1 SSL Software Compatibility

Product Number	Minimum SSL Software Version		Recommended SSL Software Version		Minimum Cisco IOS Software	Minimum Catalyst Software
SSL Services Module	Application Image	Maintenance Image	Application Image	Maintenance Image		
• WS-SVC-SSL-1 with Supervisor Engine 720	1.1(1)	1.2(1)[1]	1.2(2)	1.2(1)[1]	12.2(17a)SX1	8.2(1)
					12.2(14)SX1	–
• WS-SVC-SSL-1 with Supervisor Engine 2	1.1(1)	1.2(1)[1]	1.2(2)	1.2(1)[1]	12.1(13)E3	7.5(1)
					12.1(13)E	–

1. Do not use the 1.2(2) maintenance image

Orderable Software Images

Table 2 lists the software versions and applicable ordering information for the SSL software.

Table 2 Orderable Software Images

Software Version	Filename	Orderable Product Number
1.2(2)	c6svc-ssl-k9y9.1-2-2.bin	SC-SVC-SSL-1.2-K9
1.2(1)	c6svc-ssl-k9y9.1-2-1.bin	SC-SVC-SSL-1.2-K9
1.1(1)	c6svc-ssl-k9y9.1-1-1.bin	SC-SVC-SSL-1.1.1-K9

New Features in Software Release 1.2

This section describes the new features available in SSL software release 1.2:

- Generation of self-signed certificates for testing purposes

  You can generate multiple self-signed certificates for testing SSL proxy services by entering the **test crypto pki self** command.

- Automatic backup of configuration to NVRAM

  The Flash file system saves the entire configuration, not just the changes to the configuration. If there is a power failure during the write process, the entire configuration (including private keys) is lost. This feature automatically backs up the last saved configuration. If the current write process fails, the configuration is restored to the previous configuration automatically.

- Remove implicit VIP and VLAN binding

  This feature removes the implicit bind between virtual IP address (VIP) and VLANs.

- Support for privacy-enhanced mail (PEM) file format for importing and exporting key pairs and certificates

- SSL session timeout/session cache size

  If a session ID is found in the session cache table, the client and server can do a short handshake instead of the full handshake, which reduces the handshake overhead. The SSL **timeout session** and **session-cache size** subcommands allow you to configure how long an entry stays in the session cache and the session-cache size.

- TCP reassembly timeout

  The TCP reassembly timeout feature drops connections that reside in the reassembly queue for a extended period of time. This feature is enabled by default. If connections do not complete reassembly within a set period of time (the default is 60 seconds), they are marked and dropped to free up resources.

- Manual certificate enrollment (TFTP and cut-and-paste)

  The manual certificate enrollment (TFTP and cut-and-paste) feature allows you to generate a certificate request and accept certificate authority certificates as well as the router's certificates; these tasks are accomplished through a TFTP server or manual cut-and-paste operations.

- Up to eight levels of certificate authority

  This feature allows you to use a certificate authority of three or more levels.

- CiscoView Device Manager for Cisco Catalyst 6500 Series SSL SM 1.0 (CVDM-SSLSM)

  CVDM-SSLSM enables users to easily configure Secure Socket Layer (SSL) services on their SSL services module. It is a task-based tool that allows users to take advantage of the versatility of their SSL services module. It offers configuration wizards based on best practices in tasks such as setting up Trustpoints and proxy services.

  To access all CiscoView Device Manager documentation, go to this URL:

  http://www.cisco.com/go/cvdm

Features in Software Release 1.1

Table 3 describes the initial feature set in SSL software release 1.1.

Table 3 Feature Set Description

Features
Supported Hardware
Supervisor Engine 2 with MSFC2[1] and PFC2[2]
Supported Software
– Cisco IOS Release 12.1(13)E on the MSFC2
– Cisco IOS Release 12.1(13)E3 on the MSFC2 and Catalyst software release 7.5(1) on the Supervisor Engine 2
– SSL Services Module software release 1.1(1) on the SSL Services Module
Handshake Protocol
SSL 3.0
SSL 3.1/TLS 1.0
SSL 2.0 (only ClientHello support)
Session reuse
Session renegotiation
Symmetric Algorithms
ARC4
DES
3DES
Asymmetric Algorithms
RSA
Hash Algorithms
MD5
SHA1

Table 3 Feature Set Description (continued)

Features
Cipher Suites
SSL_RSA_WITH_RC4_128_MD5
SSL_RSA_WITH_RC4_128_SHA
SSL_RSA_WITH_DES_CSC_SHA
SSL_RSA_WITH_3DES_EDE_CBC_SHA
Public Key Infrastructure
RSA key pair generation for server certificates
Secure server key storage in SSL Services Module Flash memory device
Server certificate enrollment
Importing and exporting of server key and certificate
Duplicating keys and certificates on standby SSL Services Module using the key and certificate import and export mechanism
Manual key archival, recovery, and backup
Key and certificate renewal through the CLI
Graceful rollover of expiring server keys and certificates
Automatic enrollment of server certificates
TCP Termination
RFC 1323
Connection aging
Connection rate
Up to 64,000 concurrent client connections
Up to 192,000 concurrent connections (includes 2 MSL[3])
Up to 300 Mbps throughput
NAT[4]
Client NAT
Server NAT/PAT[5]
Scalability
Multiple modules in a single chassis when used with the CSM[6]; the CSM provides server load balancing
High Availability
Failure detection (SLB[7] health monitoring schemes)
System-level redundancy (stateless) (when used with the CSM)
Module-level redundancy (stateless) (when used with the CSM)
Serviceability
OIR[8] (after proper shutdown)
Graceful shutdown

Table 3 Feature Set Description (continued)

Features
Statistics and Accounting
Total SSL connections attempt per virtual server
Total SSL connections successfully established per virtual server
Total SSL connections failed per virtual server
Total SSL alert errors per virtual server
Total SSL resumed sessions per virtual server
Total encrypted/decrypted packets/bytes per virtual server
Configuration and Management
Direct connection to the module console port
Secure Shell (SSHv1) session
Telnet
System Capacity and Performance
Up to 300 Mbps throughput
Up to 256 proxy servers
Up to 64,000 simultaneous sessions
Stores up to 356 key pairs
Stores up to 356 certificates
Supports the following RSA key sizes: – 512-bits – 768-bits – 1024-bits – 1536-bits – 2048-bits
Up to 3000 sessions per second

1. MSFC = Multilayer Switch Feature Card
2. PFC = Policy Feature Card
3. MSL = Maximum Segment Lifetime
4. NAT = Network Address Translation
5. PAT = Port Address Translation
6. CSM = Content Switching Module
7. SLB = Server Load Balancing
8. OIR = Online Insertion And Removal

Limitations and Restrictions

This section describes general limitations and restrictions:

- Although Cisco IOS release 12.1(13)E and later supports 4096 VLANs, the SSL software supports only the normal-range VLANs (2 through 1005). Limit the SSL Services Module configuration to the normal-range VLANs.
- The SSL software does not monitor the health of the real (HTTP) servers. If a real server goes down, the system shows that the service status is up until Cisco IOS software retries and fails ARP after the default timeout period.

  Workaround 1: If you know that the HTTP server is down, enter the **no inservice** command for the corresponding SSL proxy service.

  Workaround 2: If you are using the SSL Services Module with a Content Switching Module (CSM), configure health monitoring on the CSM. (CSCdy83210)
- The client (SSL) and server (HTTP) connections that were bound during data transfer show up as four connections in the TCP connection table if both connections are in TIME_WAIT state. (CSCdy69930)
- With an open TCP connection, when the associated SSL proxy service is deleted and configured again using the same name, the association between the SSL proxy service and the previous open TCP connection is lost. Deleting and creating the same SSL proxy service creates in a new service ID for the same service name. (CSCdy68548)
- When configuring private VLANs, the SSL Services Module VLAN must be different from the primary or secondary VLAN on the client or server. If the SSL Services Module VLAN is the same as the primary or secondary VLAN on the client or server, the SSL interface may drop the traffic coming from the private VLAN. (CSCdy86258)
- The SSL Services Module supports only one route per VLAN. If you add multiple routes using the **ssl-proxy vlan** command, only the last route entered is added. (CSCdy44647)
- In SSL software release 1.1, when saving the configuration to NVRAM, if a power failure or module reset occurs, you might lose part or all of the contents in NVRAM, including the private keys stored in the private configuration file. In SSL software release 1.2, the automatic backup of configuration to NVRAM feature resolves this limitation. (CSCdy51023)
- Do not use any routing protocols on the SSL Services Module. Although you can configure Routing Information Protocol (RIP), we do not recommend it. The module supports administrative VLAN for all management (non-SSL) traffic. (CSCdz23816)
- ARP requests at line rate to the SSL Services Module result in traceback messages being displayed, warning that the module is receiving heavy traffic in its control plane, which is not a normal condition. Avoid sending wire-speed traffic to a services module. (CSCdz36033)
- The SSL Services Module is not Federal Information Processing Standards (FIPS) certified in SSL software release 1.*x*.
- If there is more than one level of certificate authority, only the lowest level certificate authority trustpoint that is authenticated and enrolled is exported in PEM files.

  Workaround: Export the enrolled trustpoint to a PKCS12 file. All levels of CA trustpoints in the certificate chain will be automatically included in the same file. (CSCea75462)

Open and Resolved Caveats in Software Release 1.2(2)

These sections describe open and resolved caveats in SSL software release 1.2(2):

Open Caveats in Release 1.2(2)

This section describes open caveats for the SSL Services Module software release 1.2(2).

- When you save your configuration using the **copy system:running-config nvram:startup-config** command with the **/erase** option, both the current and the backup buffers in NVRAM are erased before the running configuration is saved into NVRAM. If a power failure or reboot occurs after the buffers are erased but before the running configuration is saved, both configurations could be lost.

  Workaround: Do not enter the **/erase** option. (CSCea90674)

  Note If you do not enter the **/erase** option, part of the old private configuration file might remain in NVRAM.

- When you upgrade the maintenance partition image to version 1.2(1) using the application partition image version 1.2(1), an “upgrade failed” message might be displayed on the console. However, the maintenance partition image upgrades successfully. (CSCin43421)
- Importing a self-signed certificate with the key pair of the issuer is not supported by the IOS PKI system. (CSCea48145)
- Windows 2000 certificate authorities occasionally reject certificate enrollment requests issued by the SSL Services Module. The problem originated with the SCEP DLL, and is fixed on the .net version of the certificate authority, but not on the Windows 2000 version.

  Workaround: Restart the certificate authority, and issue the enrollment request again. (CSCea53069)
- When you run the cryptographic self-test, run-time performance is impacted. Run the self-test to troubleshoot persistent failures in cryptographic operations. When you finish troubleshooting, stop the test. If you run the cryptographic self-test continuously for more than three days, the system could exhaust memory and fail to set up new connections or forward traffic under heavy loads.

  Workaround: Reboot the system to regain the memory. (CSCed39184)
- If you attempt to upgrade the software image on an SSL Services Module through the main console and with a Telnet session simultaneously, the upgrade may not succeed. (CSCdy87947)
- TACACS authentication is not supported on the SSL Services Module. (CSCea76618)
- There is no help string for the **test crypto pki self** command, and the generated self-signed certificate is not displayed by the **show crypto ca certificate** command. (CSCea50887)

- The Cisco IOS PKI system cannot recover from an authentication failure, which results in a failed enrollment.

  Workaround: Enter the **no crypto ca trustpoint** *trustpoint-label* command to remove the trustpoint, and then redefine it. Make sure authentication is successful the first time, and then enroll the router certificate. (CSCea71882)

- The Cisco IOS PKI system does not validate the issuer when using manual enrollment. As a result, a certificate chain may have a root certificate belonging to one certificate authority and a router certificate issued by another certificate authority. (CSCea57072)

- For manual certificate enrollment, if the URL string ends with a backslash (/) after the TFTP server name or address (for example, tftp://ipaddress/), the system tries to open a file named ".ca" from the TFTP server.

  Workaround: Specify the filename in the URL. (CSCea32058)

- If you import a key pair and a self-signed certificate from a PKCS#12 file to a trustpoint and assign the certificate to a proxy service, installation of the certificate fails after rebooting the system, and the proxy service remains in the "no cert" state.

  Workaround: After you reboot, delete the trustpoint and import the PKCS#12 file again. The proxy service automatically reinstalls the self-signed certificate. (CSCdz20220)

- If you cut and paste the hexadecimal values of a certificate into the configuration from the terminal, the data entry might fail.

  Workaround: Copy the configuration file to the running-configuration, or import the certificate with the key pair using a PKCS#12 file. (CSCdz63758)

- When you upgrade the image, any filename in accepted with the **copy tftp: pclc#***mod***-fs:** command. There is no image name validation while upgrading the maintenance partition from the application partition or upgrading the application partition from the maintenance partition. For example, if you attempt to upgrade the application partition after booting the module in the application partition, the upgrade fails. (CSCdz23639)

- Cisco Discovery Protocol (CDP) is not supported on the SSL Services Module, however, the CLI is available. (CSCdz24446)

- The module might take longer to boot up if there are client NAT pools in the startup-configuration. The delay is proportional to the number of NAT pools in the configuration. With the maximum supported number of NAT pools (64), the delay is up to 4 minutes. (CSCdy56573)

- The time to export a PKCS#12 file using FTP can take up to 20 minutes if a file with the same name exists on the remote host. (CSCdy85233)

- When query mode is configured and there are multiple trustpoints using the same certificate authority URL, only one of these trustpoints succeeds in obtaining the whole certificate chain after a Cisco IOS reboot.

  Workaround: Manually authenticate and enroll these trustpoints after the failure. Turn off query mode and save the certificates in the NVRAM. (CSCdz03802)

- When you boot up, syslog messages indicating that proxy services are in the UP state may not be printed for all the services configured in the system. (CSCdy61618)

- Do not configure the internal port Ethernet0/0. Any configuration on Ethernet0/0 results in unexpected behavior of the SSL Services Module. (CSCdy72229)
- If you enter the **clear arp** command on the SSL Services Module, all the proxy services go down, and then come up. (CSCdy77843)
- When query mode is configured, when you enter the **no crypto ca certificate query** command on the running configuration, periodic polling for certificates does not stop. (CSCdy46075)
- When certificate query mode is configured, an "invalid input" message may be displayed on the console following a fingerprint. This message is displayed when a certificate is read from NVRAM on a Cisco IOS reboot and does not indicate a real error condition. (CSCdy43112)
- The **exportable** option in the **crypto ca import** *trustpoint_label* **pem exportable terminal** *passphrase* command does not work. The key pair is not marked as exportable after the import operation succeeds. (CSCed43692)

Resolved Caveats in Release 1.2(2)

This section describes resolved caveats in SSL Services Module software release 1.2(2):

- During a large data transfer (for example, 256 KB), the SSL Services Module might advertise the TCP window size as zero. In this case, the peer cannot send any more data to the SSL Services Module. The data transfer stops and the transaction might not be completed as expected.

  This problem is resolved in SSL software release 1.2(2). (CSCeb55184)
- On systems running Catalyst operating software on the supervisor engine, you might not be able to session to the SSL Services Module, and the module might not recover from a software reset.

  This problem is resolved in SSL software release 1.2(2). (CSCeb17020)
- Making a Telnet connection from supervisor engine console to the administration VLAN IP address on the SSL Services Module does not work. This problem exists in SSL software 1.1(1) and 1.2(1).

  Workaround 1: Enter the **session slot** *slot-number* **proc 1** command to session from the supervisor engine console to the SSL Services Module.

  Workaround 2: On the MSFC, enter the **ip telnet tos 0** command. You can then make a Telnet connection to the SSL Serices Module.

  This problem is resolved in SSL software release 1.2(2). (CSCdy81460)
- The output from the **show ssl-proxy stats ssl** command shows the overload drops counter incrementing even though the SSL Services Module is not overloaded. The SSL Services Module then rejects all connections. This situation occurs if the SSL record header spans across multiple TCP segments.

  This problem is resolved in SSL software release 1.2(2). (CSCeb83024)

Open and Resolved Caveats in Software Release 1.2(1)

These sections describe open and resolved caveats in SSL software release 1.2(1):

Open Caveats in Release 1.2(1)

This section describes open caveats for the SSL Services Module software release 1.2(1).

- When you save your configuration using the **copy system:running-config nvram:startup-config** command with the **/erase** option, both the current and the backup buffers in NVRAM are erased before the running configuration is saved into NVRAM. If a power failure or reboot occurs after the buffers are erased but before the running configuration is saved, both configurations could be lost.

  Workaround: Do not enter the **/erase** option. (CSCea90674)

  Note If you do not enter the **/erase** option, part of the old private configuration file might remain in NVRAM.

- When you upgrade the maintenance partition image to version 1.2(1) using the application partition image version 1.2(1), an “upgrade failed” message might be displayed on the console. However, the maintenance partition image upgrades successfully. (CSCin43421)
- Importing a self-signed certificate with the key pair of the issuer is not supported by the IOS PKI system. (CSCea48145)
- Windows 2000 certificate authorities occasionally reject certificate enrollment requests issued by the SSL Services Module. The problem originated with the SCEP DLL, and is fixed on the .net version of the certificate authority, but not on the Windows 2000 version.

  Workaround: Restart the certificate authority, and issue the enrollment request again. (CSCea53069)
- When you run the cryptographic self-test, run-time performance is impacted. Run the self-test to troubleshoot persistent failures in cryptographic operations. When you finish troubleshooting, stop the test. If you run the cryptographic self-test continuously for more than three days, the system could exhaust memory and fail to set up new connections or forward traffic under heavy loads.

  Workaround: Reboot the system to regain the memory. (CSCed39184)
- If you attempt to upgrade the software image on an SSL Services Module through the main console and with a Telnet session simultaneously, the upgrade may not succeed. (CSCdy87947)
- TACACS authentication is not supported in SSL Services Module. (CSCea76618)
- If there is more than one level of certificate authority, only the lowest level certificate authority trustpoint that is authenticated and enrolled is exported in PEM files.

  Workaround: Export the enrolled trustpoint to a PKCS12 file. All levels of CA trustpoints in the certificate chain will be automatically included in the same file. (CSCea75462)
- There is no help string for the **test crypto pki self** command, and the generated self-signed certificate is not displayed by the **show crypto ca certificate** command. (CSCea50887)

- The Cisco IOS PKI system cannot recover from an authentication failure, which results in a failed enrollment.

  Workaround: Enter the **no crypto ca trustpoint** *trustpoint-label* command to remove the trustpoint, and then redefine it. Make sure authentication is successful the first time, and then enroll the router certificate. (CSCea71882)

- The Cisco IOS PKI system does not validate the issuer when using manual enrollment. As a result, a certificate chain may have a root certificate belonging to one certificate authority and a router certificate issued by another certificate authority. (CSCea57072)

- For manual certificate enrollment, if the URL string ends with a backslash (/) after the TFTP server name or address (for example, tftp://ipaddress/), the system tries to open a file named ".ca" from the TFTP server.

  Workaround: Specify the filename in the URL. (CSCea32058)

- If you import a key pair and a self-signed certificate from a PKCS#12 file to a trustpoint and assign the certificate to a proxy service, installation of the certificate fails after rebooting the system, and the proxy service remains in the "no cert" state.

  Workaround: After you reboot, delete the trustpoint and import the PKCS#12 file again. The proxy service automatically reinstalls the self-signed certificate. (CSCdz20220)

- If you cut and paste the hexadecimal values of a certificate into the configuration from the terminal, the data entry might fail.

  Workaround: Copy the configuration file to the running-configuration, or import the certificate with the key pair using a PKCS#12 file. (CSCdz63758)

- When you upgrade the image, any filename in accepted with the **copy tftp: pclc#***mod***-fs:** command. There is no image name validation while upgrading the maintenance partition from the application partition or upgrading the application partition from the maintenance partition. For example, if you attempt to upgrade the application partition after booting the module in the application partition, the upgrade fails. (CSCdz23639)

- Cisco Discovery Protocol (CDP) is not supported on the SSL Services Module, however, the CLI is available. (CSCdz24446)

- The module might take longer to boot up if there are client NAT pools in the startup-configuration. The delay is proportional to the number of NAT pools in the configuration. With the maximum supported number of NAT pools (64), the delay is up to 4 minutes. (CSCdy56573)

- The time to export a PKCS#12 file using FTP can take up to 20 minutes if a file with the same name exists on the remote host. (CSCdy85233)

- When query mode is configured and there are multiple trustpoints using the same certificate authority URL, only one of these trustpoints succeeds in obtaining the whole certificate chain after a Cisco IOS reboot. (CSCdz03802)

- **Workaround**: Manually authenticate and enroll these trustpoints after the failure. Turn off query mode and save the certificates in the NVRAM.

- When you boot up, syslog messages indicating that proxy services are in the UP state may not be printed for all the services configured in the system. (CSCdy61618)

- Do not configure the internal port Ethernet0/0. Any configuration on Ethernet0/0 results in unexpected behavior of the SSL Services Module. (CSCdy72229)
- If you enter the **clear arp** command on the SSL Services Module, all the proxy services go down, and then come up. (CSCdy77843)
- When query mode is configured, entering the **no crypto ca certificate query** command on the running configuration does not stop the periodic polling for certificates. (CSCdy46075)
- When certificate query mode is configured, an "invalid input" message may be displayed on the console following a fingerprint. This message is displayed when a certificate is read from NVRAM on Cisco IOS reboot and does not indicate a real error condition. (CSCdy43112)
- The **exportable** option in the **crypto ca import** *trustpoint_label* **pem exportable terminal** *passphrase* command does not work. The key pair is not marked as exportable after the import operation succeeds. (CSCed43692)

Resolved Caveats in Release 1.2(1)

This section describes resolved caveats in SSL Services Module software release 1.2(1):

- Cisco IOS software supports only 1-tiered or 2-tiered certificate authority hierarchies.

  This problem is resolved in SSL software release 1.2(1). (CSCdy52285)
- Cisco devices that run Cisco IOS software that contains support for the Secure Shell (SSH) server are vulnerable to a denial of service (DoS) attack if the SSH server is enabled on the device.

  This vulnerability is documented as Cisco caveat ID CSCdz60229. There are workarounds available to mitigate the vulnerability. An advisory is posted at this URL:

  http://www.cisco.com/warp/public/707/ssh-packet-suite-vuln.shtml

  This problem is resolved in SSL software release 1.2(1). (CSCdz60229)
- Copying a file from a remote server to the running-configuration file using secure file transfer (SCP) sometimes fails with error 26 (internal error). This problem occurs when the remote server is running the Linux operating system.

  Workaround: Use another file transfer method (FTP or TFTP).

  This problem is resolved in SSL software release 1.2(1). (CSCdz15807)
- If the certificate authority is not reachable during authentication, traceback messages are displayed.

  Workaround: Verify that the certificate authority is reachable through the administrative VLAN from the module before doing authentication or enrollment.

  This problem is resolved in SSL software release 1.2(1). (CSCdx46916)

Open and Resolved Caveats in Software Release 1.1(1)

These sections describe open and resolved caveats in SSL software release 1.1(1):

- Open Caveats in Release 1.1(1), page 14
- Resolved Caveats in Release 1.1(1), page 15

Open Caveats in Release 1.1(1)

This section describes open caveats for the SSL Services Module software release 1.1(1).

- Cisco devices that run Cisco IOS software that contains support for the Secure Shell (SSH) server are vulnerable to a denial of service (DoS) attack if the SSH server is enabled on the device.

  This vulnerability is documented as Cisco caveat ID CSCdz60229. There are workarounds available to mitigate the vulnerability. An advisory is posted at this URL:

  http://www.cisco.com/warp/public/707/ssh-packet-suite-vuln.shtml

  (CSCdz60229)

- Cisco IOS software supports only 1-tiered or 2-tiered certificate authority hierarchies. (CSCdy52285)

- When you run the cryptographic self-test, run-time performance is impacted. Run the self-test to troubleshoot persistent failures in cryptographic operations. When you finish troubleshooting, stop the test. If you run the cryptographic self-test continuously for more than three days, the system could exhaust memory and fail to set up new connections or forward traffic under heavy loads.

  Workaround: Reboot the system to regain the memory. (CSCed39184)

- If you attempt to upgrade the software image on an SSL Services Module through the main console and with a Telnet session simultaneously, the upgrade may not succeed. (CSCdy87947)

- If you import a key pair and a self-signed certificate from a PKCS#12 file to a trustpoint and assign the certificate to a proxy service, installation of the certificate fails after rebooting the system, and the proxy service remains in the “no cert” state.

  Workaround: After you reboot, delete the trustpoint and import the PKCS#12 file again. The proxy service automatically reinstalls the self-signed certificate. (CSCdz20220)

- If you copy a file from a remote server to the running-configuration file using secure file transfer (SCP), the copy process sometimes fails with error 26 (internal error). This problem occurs when the remote server is running the Linux operating system.

  Workaround: Use another file transfer method (FTP or TFTP). (CSCdz15807)

- If you cut and paste the hexadecimal values of a certificate into the configuration from the terminal, the data entry might fail.

  Workaround: Copy the configuration file to the running-configuration, or import the certificate with the key pair using a PKCS#12 file. (CSCdz63758)

- When you upgrade the image, any filename in accepted with the **copy tftp: pclc#***mod***-fs:** command. There is no image name validation while upgrading the maintenance partition from the application partition or upgrading the application partition from the maintenance partition. For example, if you attempt to upgrade the application partition after booting the module in the application partition, the upgrade fails. (CSCdz23639)

- Cisco Discovery Protocol (CDP) is not supported on the SSL Services Module, however, the CLI is available. (CSCdz24446)

- The module might take longer to boot up if there are client NAT pools in the startup-configuration. The delay is proportional to the number of NAT pools in the configuration. With the maximum supported number of NAT pools (64), the delay is up to 4 minutes. (CSCdy56573)

- The time to export a PKCS#12 file using FTP can take up to 20 minutes if a file with the same name exists on the remote host. (CSCdy85233)

- When query mode is configured and there are multiple trustpoints using the same certificate authority URL, only one of these trustpoints succeeds in obtaining the whole certificate chain after a Cisco IOS software reboot. (CSCdz03802)

  Workaround: Manually authenticate and enroll these trustpoints after the failure. Turn off query mode and save the certificates in the NVRAM.

- If the certificate authority is not reachable during authentication, traceback messages are displayed. (CSCdx46916)

  Workaround: Verify that the certificate authority is reachable through the administrative VLAN from the module before doing authentication or enrollment.

- When you boot up, syslog messages indicating that proxy services are in the UP state may not be printed for all the services configured in the system. (CSCdy61618)
- Do not configure the internal port Ethernet0/0. Any configuration on Ethernet0/0 results in unexpected behavior of the SSL Services Module. (CSCdy72229)
- If you enter the **clear arp** command on the SSL Services Module, all the proxy services go down, and then come up. (CSCdy77843)
- When query mode is configured, if you enter the **no crypto ca certificate query** command on the running configuration, the periodic polling for certificates does not stop. (CSCdy46075)
- When certificate query mode is configured, an "invalid input" message may be displayed on the console following a fingerprint. This message is displayed when a certificate is read from NVRAM on Cisco IOS software reboot and does not indicate a real error condition. (CSCdy43112)

Resolved Caveats in Release 1.1(1)

There are no resolved caveats in SSL Services Module software release 1.1(1).

Related Documentation

For additional information about Catalyst 6500 series switches and command-line interface (CLI) commands, refer to the following:

- *Site Preparation and Safety Guide*
- *Regulatory Compliance and Safety Information for the Catalyst 6500 Series Switches*
- *Catalyst 6500 Series Switch Installation Guide*
- *Catalyst 6500 Series Switch Module Installation Guide*
- *Catalyst 6500 Series Switch Software Configuration Guide*
- *Catalyst 6500 Series Switch Command Reference*
- *Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide*
- *Catalyst 6500 Series Switch Cisco IOS Command Reference*
- *System Message Guide—Catalyst 6500 Series, 5000 Family, 4000 Family, 2926G Series, 2948G, and 2980G Switches*
- *Release Notes for Cisco IOS Release 12.1E on the Catalyst 6500 and Cisco 7600 Supervisor Engine and MSFC*
- For information about MIBs, refer to this URL:

  http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com/cisco/web/psa/default.html?mode=prod

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

http://www.cisco.com/web/siteassets/locator/index.html

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/en/US/ordering/index.shtml

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit e-mail comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour-a-day, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance. If you do not hold a valid Cisco service contract, please contact your reseller.

Cisco TAC Website

The Cisco TAC website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year. The Cisco TAC website is located at this URL:

http://www.cisco.com/tac

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

http://tools.cisco.com/RPF/register/register.do

Opening a TAC Case

Using the online TAC Case Open Tool is the fastest way to open P3 and P4 cases. (P3 and P4 cases are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using the recommended resources, your case will be assigned to a Cisco TAC engineer. The online TAC Case Open Tool is located at this URL:

https://tools.cisco.com/RPF/register/register.do

For P1 or P2 cases (P1 and P2 cases are those in which your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete listing of Cisco TAC contacts, go to this URL:

http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Go to this URL to visit the company store:

  http://www.cisco.com/go/marketplace/

- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

  http://www.cisco.com/en/US/products/index.html

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/web/about/ac123/ac114/about_cisco_packet_magazine.html

- *iQ Magazine* is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives.

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/web/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

  http://www.cisco.com/web/learning/index.html

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.