



Release Notes for the Cisco Catalyst Blade Switch 3040 for FSC, Cisco IOS Release 12.2(37)SE and Later

Revised August 8, 2007

Cisco IOS Release 12.2(37)SE and later run on the Cisco Catalyst Blade Switch 3040 for FSC, referred to as the *switch*. The switch is installed in the Fujitsu Siemens Computers (FSC) PRIMERGY BX600 system, referred to as the *BX600 system*.



Note

Before you install the switch in the BX600 system, upgrade the BX600 system management software to version 1.68 or later for the switch to operate properly.

Check for updates to this document at this URL for information about compatibility with the BX600 system software:

http://www.cisco.com/en/US/products/ps8743/prod_release_notes_list.html

These release notes include important information about Cisco IOS Release 12.2(37)SE and any limitations, restrictions, and caveats that apply to them. Verify that these release notes are correct for your switch:

- If you are installing a new switch, see the Cisco IOS release label on the switch packaging.
- If your switch is on, use the **show version** privileged EXEC command. See the “[Finding the Software Version and Feature Set](#)” section on page 3.
- If you are upgrading to a new release, see the software upgrade filename for the software version. See the “[Deciding Which Files to Use](#)” section on page 3.

For the complete list of Cisco Catalyst Blade Switch 3040 for FSC documentation, see the “[Related Documentation](#)” section on page 18.

You can download the switch software from this site (registered Cisco.com users with a login password):

<http://www.cisco.com/kobayashi/sw-center/sw-lan.shtml>

This software release is part of a special release of Cisco IOS software that is not released on the same 8-week maintenance cycle that is used for other platforms. As maintenance releases and future software releases become available, they will be posted to Cisco.com in the Cisco IOS software area.



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

© 2007 Cisco Systems, Inc. All rights reserved.

Contents

This information is in the release notes:

- [“System Requirements” section on page 2](#)
- [“Upgrading the Switch Software” section on page 3](#)
- [“Installation Notes” section on page 6](#)
- [“New Software Features” section on page 6](#)
- [“Limitations and Restrictions” section on page 6](#)
- [“Important Notes” section on page 11](#)
- [“Open Caveats” section on page 12](#)
- [“Resolved Caveats” section on page 14](#)
- [“Documentation Updates” section on page 18](#)
- [“Related Documentation” section on page 18](#)
- [“Obtaining Documentation, Obtaining Support, and Security Guidelines” section on page 19](#)

System Requirements

The system requirements are described in these sections:

- [“Hardware Supported” section on page 2](#)
- [“Device Manager System Requirements” section on page 2](#)

Hardware Supported

The hardware supported on this release is the Cisco Catalyst Blade Switch 3040 for FSC.

Device Manager System Requirements

These sections describes the hardware and software requirements for using the device manager:

- [“Hardware Requirements” section on page 2](#)
- [“Software Requirements” section on page 3](#)

Hardware Requirements

Table 1 lists the minimum hardware requirements for running the device manager.

Table 1 Minimum Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
Intel Pentium II ¹	64 MB ²	256	1024 x 768	Small

1. We recommend Intel Pentium 4.
2. We recommend 256-MB DRAM.

Software Requirements

Table 2 lists the supported operating systems and browsers for using the device manager, which does not require a plug-in. The device manager verifies the browser version when starting a session to ensure that the browser is supported.



Note

Windows NT and Windows 98 are no longer supported.

Table 2 Supported Operating Systems and Browsers

Operating System	Minimum Service Pack or Patch	Microsoft Internet Explorer ¹	Netscape Navigator
Windows 2000	None	5.5 or 6.0	7.1
Windows XP	None	5.5 or 6.0	7.1

1. Service Pack 1 or higher is required for Internet Explorer 5.5.

Upgrading the Switch Software

These are the procedures for downloading software. Before downloading software, read this section for important information:

- [“Finding the Software Version and Feature Set” section on page 3](#)
- [“Deciding Which Files to Use” section on page 3](#)
- [“Upgrading a Switch by Using the Device Manager” section on page 4](#)
- [“Upgrading a Switch by Using the CLI” section on page 5](#)
- [“Recovering from a Software Failure” section on page 6](#)

Finding the Software Version and Feature Set

The Cisco IOS image is stored as a bin file in a directory that is named with the Cisco IOS release. A subdirectory contains the files needed for web management. The image is stored on the system board flash device (flash:).

You can use the **show version** privileged EXEC command to see the software version that is running on your switch. The second line of the display shows the version.

You can also use the **dir filesystem:** privileged EXEC command to see the directory names of other software images that you might have stored in flash memory.

Deciding Which Files to Use

The upgrade procedures in these release notes describe how to perform the upgrade by using a combined tar file. This file contains the Cisco IOS image file and the files needed for the embedded device manager. You must use the combined tar file to upgrade the switch through the device manager. To upgrade the switch through the CLI, use the tar file and the **archive download-sw** privileged EXEC command.

Table 3 lists the filenames for this software release.

Table 3 Cisco IOS Software Image Files

Filename	Description
cbs40x0-lanbase-tar.122-37.SE1.tar	Cisco Catalyst Blade Switch 3040 for FSC image file and device manager files. This image has Layer 2+ features.
cbs40x0-lanbasek9-tar.122-37.SE1.tar	Cisco Catalyst Blade Switch 3040 for FSC cryptographic image file and device manager files. This image has the Kerberos and SSH features.

Archiving Software Images

Before upgrading your switch software, make sure that you have archived copies of the current Cisco IOS release and the Cisco IOS release to which you are upgrading. You should keep these archived images until you have upgraded all devices in the network to the new Cisco IOS image and until you have verified that the new Cisco IOS image works properly in your network.

Cisco routinely removes old Cisco IOS versions from Cisco.com. See *Product Bulletin 2863* for more information:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/prod_bulletin0900aecd80281c0e.html

You can copy the bin software image file on the flash memory to the appropriate TFTP directory on a host by using the **copy flash: tftp:** privileged EXEC command.



Note

Although you can copy any file on the flash memory to the TFTP server, it is time consuming to copy all of the HTML files in the tar file. We recommend that you download the tar file from Cisco.com and archive it on an internal host in your network.

You can also configure the switch as a TFTP server to copy files from one switch to another without using an external TFTP server by using the **tftp-server** global configuration command. For more information about the **tftp-server** command, see the “Basic File Transfer Services Commands” section of the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2* at this URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_book09186a00800811e0.html

Upgrading a Switch by Using the Device Manager

You can upgrade switch software by using the device manager. For detailed instructions, click **Help**.



Note

When using the device manager to upgrade your switch, do not use or close your browser session after the upgrade process begins. Wait until after the upgrade process completes.

Upgrading a Switch by Using the CLI

This procedure is for copying the combined tar file to the switch. You copy the file to the switch from a TFTP server and extract the files. You can download an image file and replace or keep the current image.

To download software, follow these steps:

-
- Step 1** Use [Table 3 on page 4](#) to identify the file that you want to download.
- Step 2** Download the software image file. If you have a SmartNet support contract, go to this URL, and log in to download the appropriate files:

<http://www.cisco.com/kobayashi/sw-center/sw-lan.shtml>

- Step 3** Copy the image to the appropriate TFTP directory on the workstation, and make sure that the TFTP server is properly configured.

For more information, see Appendix B in the software configuration guide for this release.

- Step 4** Log into the switch through the console port or a Telnet session.

- Step 5** (Optional) Ensure that you have IP connectivity to the TFTP server by entering this privileged EXEC command:

```
Switch# ping tftp-server-address
```

For more information about assigning an IP address and default gateway to the switch, see the software configuration guide for this release.

- Step 6** Download the image file from the TFTP server to the switch. If you are installing the same version of software that is currently on the switch, overwrite the current image by entering this privileged EXEC command:

```
Switch# archive download-sw /overwrite /reload
tftp:[[/location]/directory]/image-name.tar
```

The **/overwrite** option overwrites the software image in flash memory with the downloaded one.

The **/reload** option reloads the system after downloading the image unless the configuration has been changed and not saved.

For *//location*, specify the IP address of the TFTP server.

For */directory/image-name.tar*, specify the directory (optional) and the image to download. Directory and image names are case sensitive.

This example shows how to download an image from a TFTP server at 198.30.20.19 and to overwrite the image on the switch:

```
Switch# archive download-sw /overwrite
tftp://198.30.20.19/c3750-ipservices-tar.122-35.SE.tar
```

You can also download the image file from the TFTP server to the switch and keep the current image by replacing the **/overwrite** option with the **/leave-old-sw** option.

Recovering from a Software Failure

For additional recovery procedures, see the “Troubleshooting” chapter in the software configuration guide for this release.

Installation Notes

You can assign IP information to your switch by using these methods:

- The Express Setup program or the HP Onboard Administrator program described in the getting started guide.
- The CLI-based setup program, as described in the hardware installation guide.
- The DHCP-based autoconfiguration, as described in the software configuration guide.
- Manually assigning an IP address, as described in the software configuration guide.

New Software Features

These are the new software features for this release:

- VLAN Flex Links load balancing to configure a Flex Links pair to allow both ports to forward traffic for some VLANs (mutually exclusive)
- Link Layer Discovery Protocol (LLDP) and LLDP Media Endpoint Discovery (LLDP-MED) for interoperability with third-party IP phones
- VLAN aware port security option to shut down the VLAN on the port when a violation occurs, instead of shutting down the entire port
- DHCP Snooping Statistics **show** and **clear** commands to display and remove DHCP snooping statistics in summary or detail form
- SNMP support for the Port Error Disable MIB
- Support for the Time Domain Reflectometry MIB

Limitations and Restrictions

You should review this section before you begin working with the switch. These are known limitations that will not be fixed, and there is not always a workaround. Some features might not work as documented, and some features could be affected by recent changes to the switch hardware or software.

This section contains these limitations:

- [“Cisco IOS Limitations” section on page 7](#)
- [“Device Manager Limitations” section on page 11](#)

Cisco IOS Limitations

These limitations apply to the switch:

- “Configuration” section on page 7
- “Ethernet” section on page 8
- “IP” section on page 8
- “IP Telephony” section on page 8
- “MAC Addressing Multicasting” section on page 8
- “MAC Addressing Multicasting” section on page 8
- “QoS” section on page 9
- “SPAN and RSPAN” section on page 10
- “Trunking” section on page 10
- “VLAN” section on page 10

Configuration

These are the configuration limitations:

- A static IP address might be removed when the previously acquired DHCP IP address lease expires.

This problem occurs under these conditions:

- When the switch is booted without a configuration (no config.text file in flash memory).
- When the switch is connected to a DHCP server that is configured to give an address to it (the dynamic IP address is assigned to VLAN 1).
- When an IP address is configured on VLAN 1 before the dynamic address lease assigned to VLAN 1 expires.

The workaround is to reconfigure the static IP address. (CSCea71176 and CSCdz11708)

- When connected to some third-party devices that send early preambles, a switch port operating at 100 Mp/s full duplex or 100 Mp/s half duplex might bounce the line protocol up and down. The problem is observed only when the switch is receiving frames.

The workaround is to configure the port for 10 Mp/s and half duplex or to connect a hub or a nonaffected device to the switch. (CSCed39091)

- When port security is enabled on an interface in restricted mode and the **switchport block unicast interface** command has been entered on that interface, MAC addresses are incorrectly forwarded when they should be blocked

The workaround is to enter the **no switchport block unicast** interface configuration command on that specific interface. (CSCee93822)

- A traceback error occurs if a crypto key is generated after an SSL client session.

There is no workaround. This is a cosmetic error and does not affect the functionality of the switch. (CSCef59331)

Ethernet

This is the Ethernet limitation:

Traffic on EtherChannel ports is not perfectly load-balanced. Egress traffic on EtherChannel ports are distributed to member ports on load balance configuration and traffic characteristics like MAC or IP address. More than one traffic stream might map to same member ports, based on hashing results calculated by the ASIC.

If this happens, traffic distribution is uneven on EtherChannel ports.

Changing the load balance distribution method or changing the number of ports in the EtherChannel can resolve this problem. Use any of these workarounds to improve EtherChannel load balancing:

- for random source-ip and dest-ip traffic, configure load balance method as **src-dst-ip**
- for incrementing source-ip traffic, configure load balance method as **src-ip**
- for incrementing dest-ip traffic, configure load balance method as **dst-ip**
- Configure the number of ports in the EtherChannel so that the number is equal to a power of 2 (for example, 2, 4, or 8)

For example, with load balance configured as **dst-ip** with 150 distinct incrementing destination IP addresses, and the number of ports in the EtherChannel set to either 2, 4, or 8, load distribution is optimal. (CSCeh81991)

IP

This is the IP limitation:

When the rate of received DHCP requests exceeds 2,000 packets per minute for a long time, the response time might be slow when you are using the console. The workaround is to use rate limiting on DHCP traffic to prevent a denial of service attack from occurring. (CSCeb59166)

IP Telephony

This is the IP telephony limitation:

After you change the access VLAN on a port that has IEEE 802.1x enabled, the IP phone address is removed. Because learning is restricted on IEEE 802.1x-capable ports, it takes approximately 30 seconds before the address is relearned. No workaround is necessary. This limitation is unlikely to affect the Cisco Catalyst Blade Switch 3040 for FSC because IP phones are not usually connected to the switch uplink ports. (CSCea85312)

MAC Addressing Multicasting

These are the multicasting limitations:

- If the number of multicast routes and Internet Group Management Protocol (IGMP) groups are more than the maximum number specified by the **show sdm prefer** global configuration command, the traffic received on unknown groups is flooded in the received VLAN even though the **show ip igmp snooping multicast-table** privileged EXEC command output shows otherwise. The workaround is to reduce the number of multicast routes and IGMP snooping groups to less than the maximum supported value. (CSCdy09008)

- IGMP filtering is applied to packets that are forwarded through hardware. It is not applied to packets that are forwarded through software. Hence, with multicast routing enabled, the first few packets are sent from a port even when IGMP filtering is set to deny those groups on that port. There is no workaround. (CSCdy82818)
- If an IGMP report packet has two multicast group records, the switch removes or adds interfaces depending on the order of the records in the packet:
 - If the `ALLOW_NEW_SOURCE` record is before the `BLOCK_OLD_SOURCE` record, the switch removes the port from the group.
 - If the `BLOCK_OLD_SOURCE` record is before the `ALLOW_NEW_SOURCE` record, the switch adds the port to the group.

There is no workaround. (CSCec20128)

- When IGMP snooping is disabled and you enter the `switchport block multicast` interface configuration command, IP multicast traffic is not blocked.

The `switchport block multicast` interface configuration command is only applicable to non-IP multicast traffic.

There is no workaround. (CSCee16865)

- Incomplete multicast traffic can be seen under either of these conditions:
 - You disable IP multicast routing or re-enable it globally on an interface.
 - A switch mroute table temporarily runs out of resources and recovers later.

The workaround is to enter the `clear ip mroute` privileged EXEC command on the interface. (CSCef42436)

After you configure a switch to join a multicast group by entering the `ip igmp join-group group-address` interface configuration command, the switch does not receive join packets from the client, and the switch port connected to the client is removed from the IGMP snooping forwarding table.

Use one of these workarounds:

- Cancel membership in the multicast group by using the `no ip igmp join-group group-address` interface configuration command on an SVI.
- Disable IGMP snooping on the VLAN interface by using the `no ip igmp snooping vlan vlan-id` global configuration command. (CSCeh90425)

QoS

These are the quality of service (QoS) limitations:

- Some switch queues are disabled if the buffer size or threshold level is set too low with the `mls qos queue-set output` global configuration command. The ratio of buffer size to threshold level should be greater than 10 to avoid disabling the queue. The workaround is to choose compatible buffer sizes and threshold levels. (CSCea76893)
- When auto-QoS is enabled on the switch, priority queuing is not enabled. Instead, the switch uses shaped round robin (SRR) as the queuing mechanism. The auto-QoS feature is designed on each platform based on the feature set and hardware limitations, and the queuing mechanism supported on each platform might be different. There is no workaround. (CSCee22591)

SPAN and RSPAN

These are the SPAN and Remote SPAN (RSPAN) limitations.

- Egress SPAN routed packets (both unicast and multicast) show the incorrect source MAC address. For remote SPAN packets, the source MAC address should be the MAC address of the egress VLAN, but instead the packet shows the MAC address of the RSPAN VLAN. For local SPAN packets with native encapsulation on the destination port, the packet shows the MAC address of VLAN 1. This problem does not appear with local SPAN when the **encapsulation replicate** option is used. This limitation does not apply to bridged packets. The workaround is to use the **encapsulate replicate** keywords in the **monitor session** global configuration command. Otherwise, there is no workaround. This is a hardware limitation. (CSCdy81521)
- During periods of very high traffic when two RSPAN source sessions are configured, the VLAN ID of packets in one RSPAN session might overwrite the VLAN ID of the other RSPAN session. If this occurs, packets intended for one RSPAN VLAN are incorrectly sent to the other RSPAN VLAN. This problem does not affect RSPAN destination sessions. The workaround is to configure only one RSPAN source session. This is a hardware limitation. (CSCea72326)
- Cisco Discovery Protocol (CDP), VLAN Trunking Protocol (VTP), and Port Aggregation Protocol (PAgP) packets received from a SPAN source are not sent to the destination interfaces of a local SPAN session. The workaround is to use the **monitor session session_number destination {interface interface-id encapsulation replicate}** global configuration command for local SPAN. (CSCed24036)

Trunking

These are the trunking limitations:

- The switch treats frames received with mixed encapsulation (IEEE 802.1Q and Inter-Switch Link [ISL]) as frames with FCS errors, increments the error counters, and the port LED blinks amber. This happens when an ISL-unaware device receives an ISL-encapsulated packet and forwards the frame to an IEEE 802.1Q trunk interface. There is no workaround. (CSCdz33708)
- IP traffic with IP options set is sometimes leaked on a trunk port. For example, a trunk port is a member of an IP multicast group in VLAN X but is not a member in VLAN Y. If VLAN Y is the output interface for the multicast route entry assigned to the multicast group and an interface in VLAN Y belongs to the same multicast group, the IP-option traffic received on an input VLAN interface other than one in VLAN Y is sent on the trunk port in VLAN Y because the trunk port is forwarding in VLAN Y, even though the port has no group membership in VLAN Y. There is no workaround. (CSCdz42909).
- For trunk ports or access ports configured with IEEE 802.1Q tagging, inconsistent statistics might appear in the **show interfaces counters** privileged EXEC command output. Valid IEEE 802.1Q frames of 64 to 66 bytes are correctly forwarded even though the port LED blinks amber, and the frames are not counted on the interface statistics. There is no workaround. (CSCec35100).

VLAN

This is the VLAN limitation:

- If the number of VLANs times the number of trunk ports exceeds the recommended limit of 13,000, the switch can fail.

The workaround is to reduce the number of VLANs or trunks. (CSCeb31087)

Device Manager Limitations

This is the device manager limitation for this release:

When you are prompted to accept the security certificate and you click *No*, you only see a blank screen, and the device manager does not start.

The workaround is to click *Yes* when you are prompted to accept the certificate. (CSCef45718)

Important Notes

These sections describe the important notes related to this software release:

- [“Cisco IOS Notes” section on page 11](#)
- [“Device Manager Notes” section on page 11](#)

Cisco IOS Notes

These notes apply to Cisco IOS software:

- The behavior of the **no logging on** global configuration command changed in Cisco IOS Release 12.2(18)SE and later. You can only use the **logging on** and then the **no logging console** global configuration commands to disable logging to the console. (CSCec71490)
- In Cisco IOS Release 12.2(25)SEC, the implementation for multiple spanning tree (MST) changed from the previous release. Multiple STP (MSTP) complies with the IEEE 802.1s standard. Previous MSTP implementations were based on a draft of the IEEE 802.1s standard.
- If the switch requests information from the Cisco Secure Access Control Server (ACS) and the message exchange times out because the server does not respond, a message similar to this appears:

```
00:02:57: %RADIUS-4-RADIUS_DEAD: RADIUS server 172.20.246.206:1645,1646 is not responding.
```

If this message appears, make sure that there is network connectivity between the switch and the ACS. You should also make sure that the switch has been properly configured as an AAA client on the ACS.

Device Manager Notes

These notes apply to the device manager:

- We recommend this browser setting to more quickly display the device manager from Microsoft Internet Explorer.

From Microsoft Internet Explorer:

1. Choose **Tools > Internet Options**.
2. Click **Settings** in the Temporary Internet files area.
3. From the Settings window, choose **Automatically**.
4. Click **OK**.
5. Click **OK** to exit the Internet Options window.

- The HTTP server interface must be enabled to display the device manager. By default, the HTTP server is enabled on the switch. Use the **show running-config** privileged EXEC command to see if the HTTP server is enabled or disabled.
- If you use Internet Explorer Version 5.5 and select a URL with a nonstandard port at the end of the address (for example, *www.cisco.com:84*), you must enter *http://* as the URL prefix. Otherwise, you cannot start the device manager.

Open Caveats

This section describes the open severity 3 Cisco IOS configuration caveats with possible unexpected activity in this software release:

- CSCsb85001

If traffic is passing through VMPS ports and you perform a **shut** operation, a dynamic VLAN is not assigned and a VLAN with a null ID appears.

The workaround is to clear the MAC address table. This forces the VMPS server to correctly reassign the VLAN.

- CSCsc30733

This error message appears during authentication when a method list is used and one of the methods in the method list is removed:

```
AAA-3-BADMETHODERROR:Cannot process authentication method 218959117
```

There is no workaround. However, this is only an informational message and does not affect switch functionality.

- CSCsc59418

A QoS service policy with a policy map containing more than 62 policers cannot be added to an interface by using the **service-policy** interface configuration command.

The workaround is to use policy maps with 62 or fewer policers.

- CSCsc96474

The switch might display tracebacks similar to these examples when a large number of IEEE 802.1x supplicants try to repeatedly log in and log out.

Examples:

```
Jan 3 17:54:32 L3A3 307: Jan 3 18:04:13.459: %SM-4-BADEVENT: Event 'eapReq' is invalid
for the current state 'auth_bend_idle': dot1x_auth_bend Fa9
```

```
Jan 3 17:54:32 L3A3 308: -Traceback= B37A84 18DAB0 2FF6C0 2FF260 8F2B64 8E912C Jan 3
19:06:13 L3A3 309: Jan 3 19:15:54.720: %SM-4-BADEVENT: Event 'eapReq_no_reAuthMax' is
invalid for the current ate 'auth_restart': dot1x_auth Fa4
```

```
Jan 3 19:06:13 L3A3 310: -Traceback= B37A84 18DAB0 3046F4 302C80 303228 8F2B64 8E912C
Jan 3 20:41:44 L3A3 315: .Jan 3 20:51:26.249: %SM-4-BADEVENT: Event 'eapSuccess' is
invalid for the current state 'auth_restart': dot1x_auth Fa9
```

```
Jan 3 20:41:44 L3A3 316: -Traceback= B37A84 18DAB0 304648 302C80 303228 8F2B64 8E912C
```

There is no workaround.

- CSCsd03580

When IEEE 802.1x is globally disabled on the switch by using the **no dot1x system-auth-control** global configuration command, some interface level configuration commands, including the **dot1x timeout** and **dot1x mac-auth-bypass commands**, become unavailable.

- The workaround is to enable the **dot1x system-auth-control** global configuration command before attempting to configure interface level IEEE 802.1x parameters.
- CSCse06827

When dynamic ARP inspection is configured on a VLAN, and the ARP traffic on a port in the VLAN is within the configured rate limit, the port might go into an error-disabled state.

The workaround is to configure the burst interval to more than 1 second.
 - CSCsg18176

When dynamic ARP inspection is enabled and IP validation is disabled, the switch drops ARP requests that have a source address of 0.0.0.0.

The workaround is to configure an ARP access control list (ACL) that permits IP packets with a source IP address of 0.0.0.0 (and any MAC) address) and apply the ARP ACL to the desired DAI VLANs.
 - CSCsg21537

When MAC addresses are learned on an Etherchannel port, the addresses are incorrectly deleted from the MAC address table even when the MAC address table aging timeout value is configured to be longer than the ARP timeout value. This causes intermittent unicast packet flooding in the network.
 - CSCsg30295

When you configure an IP address on a switch virtual interface (SVI) with DHCP and enable DHCP snooping on the SVI VLAN, the switch SVI cannot obtain an IP address.

The workaround is to not enable DHCP snooping on the SVI VLAN or to use a static IP address for the SVI.
 - CSCsg79506

During repeated reauthentication of supplicants on an IEEE 802.1x-enabled switch, if the RADIUS server is repeatedly going out of service and then coming back up, the available switch memory might deplete over time, eventually causing the switch to shut down.

There is no work-around, except to ensure that the RADIUS server is stable.
 - CSCsg81334

If IEEE 802.1x critical authentication is not enabled and the RADIUS authentication server is temporarily unavailable during a reauthentication, when the RADIUS server comes back up, MAC authentication bypass (MAB) does not authenticate a previously authenticated client.

The workaround is to enter the **shutdown** interface configuration command followed by the **no shutdown** command on the port connected to the client. An alternative, to prevent the problem from occurring, is to enable critical authentication by entering the **dot1x critical {eapol | recovery delay milliseconds}** global configuration command.
 - CSCsi63999

Changing the spanning tree mode from rapid STP to MSTP can cause tracebacks when the virtual port error-disable feature is enabled when the STP mode is changed.

There is no workaround.

- CSCsi75246

An address learned as a supplicant that is aged out by port security aging is never relearned by port security under any of these conditions:

- IEEE 802.1x authentication, port security, and port security aging are enabled on a port.
- An address is cleared by port security.
- You enter the **clear port security** privileged EXEC command.

The workaround is to use the **dot1x timeout** interface configuration command instead of the port security aging timer as the reauthentication timer for IEEE 802.

Resolved Caveats

These sections describe the caveats that have been resolved in these releases:

- [Caveats Resolved in Cisco IOS Release 12.2\(37\)SE1, page 14](#)
- [Caveats Resolved in Cisco IOS Release 12.2\(37\)SE, page 15](#)

Caveats Resolved in Cisco IOS Release 12.2(37)SE1

These caveats are resolved in Cisco IOS Release 12.2.(37)SE1:

- CSCsc19259

The server side of the Secure Copy (SCP) implementation in Cisco IOS contains a vulnerability that allows any valid user, regardless of privilege level, to transfer files to and from an IOS device that is configured to be a Secure Copy server. This vulnerability could allow valid users to retrieve or write to any file on the device's filesystem, including the device's saved configuration. This configuration file may include passwords or other sensitive information.

The Cisco IOS Secure Copy Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the Cisco IOS Secure Copy Server service are not affected by this vulnerability.

This vulnerability does not apply to the Cisco IOS Secure Copy Client feature.

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20070808-scp.shtml>.

- CSCsj13619

The SCP (Secure Copy Protocol) support is now correctly included in the image. The **show file systems** and **copy** privileged EXEC commands now correctly show **scp** as an option.

- CSCsj19641

The switch no longer drops ARP packets destined to MAC addresses that are close to the MAC address block of the switch.

Caveats Resolved in Cisco IOS Release 12.2(37)SE

These caveats are resolved in Cisco IOS Release 12.2.(37)SE:

- CSCsb12598

Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

Cisco IOS is affected by the following vulnerabilities:

- Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
- Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
- Processing Finished messages, documented as Cisco bug ID CSCsd92405

Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml>.



Note

Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml>.

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml>.

- CSCsb40304

Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

Cisco IOS is affected by the following vulnerabilities:

- Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
- Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
- Processing Finished messages, documented as Cisco bug ID CSCsd92405

Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml>.

**Note**

Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml>.

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml>.

- CSCsc30733

This error message no longer appears during authentication when a method list is used and one of the methods in the method list is removed:

```
AAA-3-BADMETHODERROR:Cannot process authentication method 218959117
```

- CSCsd60718

When you enter the **no speed** interface configuration command, the Ethernet interface speed now correctly returns to its default setting. This affects interfaces Gigabit Ethernet 0/17 to Gigabit Ethernet 0/20, Gigabit Ethernet 0/23, and Gigabit Ethernet 0/24. This does not affect interfaces Gigabit Ethernet 0/21 and Gigabit Ethernet 0/22.

- CSCsd85587

A vulnerability has been discovered in a third party cryptographic library which is used by a number of Cisco products. This vulnerability may be triggered when a malformed Abstract Syntax Notation One (ASN.1) object is parsed. Due to the nature of the vulnerability it may be possible, in some cases, to trigger this vulnerability without a valid certificate or valid application-layer credentials (such as a valid username or password).

Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

The vulnerable cryptographic library is used in the following Cisco products:

- Cisco IOS, documented as Cisco bug ID CSCsd85587
- Cisco IOS XR, documented as Cisco bug ID CSCsg41084
- Cisco PIX and ASA Security Appliances, documented as Cisco bug ID CSCse91999
- Cisco Unified CallManager, documented as Cisco bug ID CSCsg44348
- Cisco Firewall Service Module (FWSM)

This vulnerability is also being tracked by CERT/CC as VU#754281.

Cisco has made free software available to address this vulnerability for affected customers. There are no workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml>.

**Note**

Another related advisory is posted together with this Advisory. It also describes vulnerabilities related to cryptography that affect Cisco IOS. A combined software table for Cisco IOS only is available at <http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml> and can be used to choose a software release which fixes all security vulnerabilities published as of May 22, 2007. The related advisory is published at <http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml>.

- CSCsd92405

Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

Cisco IOS is affected by the following vulnerabilities:

- Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
- Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
- Processing Finished messages, documented as Cisco bug ID CSCsd92405

Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml>.

**Note**

Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link: <http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml>.

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml>.

- CSCsg18176

When dynamic ARP inspection is enabled and IP validation is disabled, the switch no longer drops ARP requests that have a source address of 0.0.0.0.

- CSCsg30295

When you configure an IP address on a switch virtual interface (SVI) with DHCP and enable DHCP snooping on the SVI VLAN, the switch SVI now obtains an IP address.

- CSCsh92834

When trunk ports are participating in a Flex Link configuration, entering a **shutdown** or **no shutdown** interface configuration command on the port no longer causes the switch to reload.

- CSCsh92844

Online insertion and removal (OIR) of an SFP module no longer causes error-disabled ports to change to Up or Standby states, resulting in lost data.

- CSCsi00879
When IGMP snooping is enabled, multicast traffic no longer is dropped after a port channel interface link flaps.
- CSCsi30888
The switch no longer halts when configuring link-state tracking with EtherChannel downstream ports or when booting up a switch already configured with link-state tracking with EtherChannel downstream ports.

Documentation Updates

This section was added to the Configuring IEEE 802.1x chapter of the software configuration guide.

Web Authentication with Automatic MAC Check

You can use web authentication with automatic MAC check to authenticate a client that does not support IEEE 802.1x or web browser functionality. This allows end hosts, such as printers, to automatically authenticate by using the MAC address without any additional required configuration.

Web authentication with automatic MAC check only works in web authentication standalone mode. You cannot use this if web authentication is configured as a fallback to IEEE 802.1x authentication.

The MAC address of the device must be configured in the Access Control Server (ACS) for the automatic MAC check to succeed. The automatic MAC check allows managed devices, such as printers, to skip web authentication.



Note

The interoperability of web authentication (with automatic MAC check) and IEEE 802.1x MAC authentication configured on different ports of the same switch is not supported.

Related Documentation

These documents provide complete information about the Cisco Catalyst Blade Switch 3040 for FSC and are available at Cisco.com:

http://www.cisco.com/en/US/products/ps8743/tsd_products_support_series_home.html

You can order printed copies of documents with a DOC-xxxxx= number from the Cisco.com sites and from the telephone numbers listed in the URL referenced in the [“Obtaining Documentation, Obtaining Support, and Security Guidelines”](#) section on page 19.

These documents provide complete information about the Cisco Catalyst Blade Switch 3040 for FSC:

- *Cisco Catalyst Blade Switch 3040 for FSC Getting Started Guide* (order number DOC-7817759=)
- *Regulatory Compliance and Safety Information for the Cisco Catalyst Blade Switch 3040 for FSC* (order number DOC-7817760=)
- *Release Notes for the Cisco Catalyst Blade Switch 3040 for FSC, Cisco IOS Release 12.2(37)SE* (not orderable but available on Cisco.com)
- *Cisco Catalyst Blade Switch 3040 for FSC Software Configuration Guide* (not orderable but available on Cisco.com)

- *Cisco Catalyst Blade Switch 3040 for FSC Command Reference* (not orderable but available on Cisco.com)
- *Cisco Catalyst Blade Switch 3040 for FSC System Message Guide* (not orderable but available on Cisco.com)

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0705R)

