

Cisco Security Advisory: Cisco Catalyst Supervisor Remote Reload

Document ID: 13650

Advisory ID: cisco-sa-19990324-cat7161

<http://www.cisco.com/warp/public/707/cisco-sa-19990324-cat7161.shtml>

Revision 1.2

For Public Release 1999 March 24 2000 UTC (GMT)

Please provide your feedback on this document.

Summary
Affected Products
Details
Impact
Software Versions and Fixes
Workarounds
Obtaining Fixed Software
Exploitation and Public Announcements
Status of This Notice: FINAL
Distribution
Revision History
Cisco Security Procedures

Summary

A software bug (Cisco bug ID CSCdi74333) allows remote TCP/IP users to cause reloads of Cisco Catalyst LAN switches running Catalyst 5000 supervisor software versions from 1.0 through 2.1(5). The affected software was last shipped with new units in early 1997. In addition to the Catalyst 5xxx series, some, but not all, Catalyst 29xx family switches may run the affected software; see "Who is Affected" for more information.

A similar bug, Cisco bug ID CSCdj71684, exists in the supervisor software for the older, and now discontinued, Catalyst 12xx family, up through software version 4.29.

Fixes are available for both bugs. The fixes have been in the field for some time. Most Catalyst switch users have probably already installed the fixes.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-19990324-cat7161.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

The following Cisco Catalyst LAN switch models are affected by this vulnerability—

- The Catalyst 12xx family, running supervisor software versions up to and including 4.29.
- The Catalyst 29xx family (but *not* the Catalyst 2900XL), running supervisor software versions up to and including 2.1(5), 2.1(501), and 2.1(502). This includes the Catalyst 2901, 2902, and 2903 switches. Catalyst 2926 switches are *not* affected, because the Catalyst 2926 was not released until after the software fix was made. Catalyst 2900XL switches run unrelated software, and are *not* affected by this vulnerability.
- The Catalyst 5xxx series (including the Catalyst 55xx family), running supervisor software versions up to and including 2.1(5), 2.1(501), and 2.1(502).

Fixed software for the Catalyst 5xxx and Catalyst 29xx series began shipping with new switches in mid-1997. Sales of the Catalyst 12xx family were stopped before the release of software version 4.30; if you have not upgraded your software since installing your Catalyst 12xx switch, you are affected by this vulnerability.

The affected Cisco Catalyst LAN switches are rack-mountable units typically found in data centers and cable closets.

Products Confirmed Not Vulnerable

Catalyst 5xxx and 29xx switches running versions 2.1(6) and later are *not* affected. Catalyst 12xx switches running versions 4.30 and later are *not* affected. Some Cisco Catalyst switches include intelligent modules that run software independent of the supervisor software. These modules, which include a variety of media controllers as well as the route switch module (RSM), are *not* affected.

No other Cisco products are currently known to be affected by these vulnerabilities.

Details

For the Catalyst 29xx and Catalyst 5xxx switches, this vulnerability has Cisco bug ID CSCdi74333. The bug is present in all supervisor software versions through 2.1(5), including the spot fix releases 2.1(501) and 2.1(502). The bug is fixed in 2.1(6) and later versions, including all 2.2, 2.3, and 2.4 versions, and all 3.x, 4.x, and later versions.

For the Catalyst 1200, this vulnerability has Cisco bug ID CSCdj71684. The bug is present in all software versions through 4.29, and is fixed in 4.30 and later versions.

Impact

A remote attacker who knows how to exploit this vulnerability, and who can make a connection to TCP port 7161 on an affected switch, can cause the supervisor module of that switch to reload. While the supervisor is reloading, the switch will not forward traffic, and the attack will therefore deny service to the equipment attached to the switch. The switch will recover automatically, but repeated attacks can extend the denial of service indefinitely.

Software Versions and Fixes

When considering software upgrades, also consult <http://www.cisco.com/go/psirt> and any subsequent

advisories to determine exposure and a complete upgrade solution.

In all cases, customers should exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, contact the Cisco Technical Assistance Center ("TAC") or your contracted maintenance provider for assistance.

Workarounds

This vulnerability may be worked around by assigning no IP addresses to affected Cisco Catalyst switches. However, this workaround will have the effect of disabling all remote management of those switches.

Another possible workaround is to use the filtering capabilities of surrounding routers and/or dedicated firewall devices to prevent untrusted hosts from making connections to TCP port 7161 on affected switches.

Obtaining Fixed Software

Cisco has made free software available to address this vulnerability for affected customers. Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

Customers may only install and expect support for the feature sets they have purchased. By installing, downloading, accessing or otherwise using such software upgrades, customers agree to be bound by the terms of Cisco's software license terms found at <http://www.cisco.com/public/sw-license-agreement.html>, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software upgrades.

Customers with Service Contracts

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's worldwide website at <http://www.cisco.com>.

Customers using Third-party Support Organizations

Customers whose Cisco products are provided or maintained through prior or existing agreement with third-party support organizations such as Cisco Partners, authorized resellers, or service providers should contact that support organization for guidance and assistance with the appropriate course of action in regards to this advisory.

The effectiveness of any workaround or fix is dependent on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. Due to the variety of affected products and releases, customers should consult with their service provider or support organization to ensure any applied workaround or fix is the most appropriate for use in the intended network before it is deployed.

Customers without Service Contracts

Customers who purchase direct from Cisco but who do not hold a Cisco service contract and customers who purchase through third-party vendors but are unsuccessful at obtaining fixed software through their point of

sale should get their upgrades by contacting the Cisco Technical Assistance Center (TAC). TAC contacts are as follows.

- +1 800 553 2447 (toll free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)
- e-mail: tac@cisco.com

Have your product serial number available and give the URL of this notice as evidence of your entitlement to a free upgrade. Free upgrades for non-contract customers must be requested through the TAC.

Refer to <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> for additional TAC contact information, including special localized telephone numbers and instructions and e-mail addresses for use in various languages.

Exploitation and Public Announcements

Cisco knows of no public announcements or discussion of this vulnerability before the date of this notice. Cisco has had no reports of malicious exploitation of this vulnerability. These bugs were identified and reported by outside companies conducting laboratory testing.

No special tools, and only the most basic of skills, are needed to exploit this vulnerability. It would not be difficult for a person with minimal sophistication to find a way to exploit this vulnerability.

Cisco thanks the Internet Security Systems (ISS) X-Force, for independently discovering this matter and bringing it to the attention of Cisco's Product Security Incident Response Team (PSIRT).

The initial report of CSCdi74333 was received before the establishment of the PSIRT, from a customer who has neither requested credit nor given permission to be named in this notice. Cisco security notices do not name or credit third parties without their specific permission.

Status of This Notice: FINAL

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

A stand-alone copy or Paraphrase of the text of this document that omits the distribution URL in the following section is an uncontrolled copy, and may lack important information or contain factual errors.

Distribution

This advisory will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-19990324-cat7161.shtml>.

In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key and is posted to the following e-mail and Usenet news recipients.

- cust-security-announce@cisco.com
- bugtraq@securityfocus.com

Cisco Security Advisory: Cisco Catalyst Supervisor Remote Reload

- first-teams@first.org (includes CERT/CC)
- Various internal Cisco mailing lists

Future updates of this advisory, if any, will be placed on Cisco's worldwide website, but may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the above URL for any updates.

Revision History

Revision 1.2	1999 March 24	Initial public release.
--------------	---------------	-------------------------

Cisco Security Procedures

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Mar 24, 1999

Document ID: 13650
