

# Cisco Security Advisory: Cisco IOS Syslog Crash

Document ID: 13660

Advisory ID: cisco-sa-19990111-ios-syslog

<http://www.cisco.com/warp/public/707/cisco-sa-19990111-ios-syslog.shtml>

## Revision 1.1

For Public Release 1999 January 11 1600 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

Certain versions of Cisco IOS software may crash or hang when they receive invalid user datagram protocol (UDP) packets sent to their "syslog" ports (port 514). At least one commonly-used Internet scanning tool generates packets which can cause such crashes and hangs. This fact has been announced on public Internet mailing lists which are widely read both by security professionals and by security "crackers", and should be considered public information.

This vulnerability affects devices running Cisco IOS software version 11.3AA, version 11.3DB, or any 12.0-based version (including 12.0 mainline, 12.0S, 12.0T, and any other regular released version whose number starts with "12.0"). The vulnerability has been corrected in certain special releases, and will be corrected in maintenance and interim releases which will be issued in the future; see the section on "Software Versions and Fixes" for details on which versions are affected, and on which versions are, or will be, fixed. Cisco intends to provide fixes for all affected IOS variants.

There is a configuration workaround for this vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-19990111-ios-syslog.shtml>.

## Affected Products

This section provides details on affected products.

## Vulnerable Products

All Cisco devices which are running classic Cisco IOS software with any of the versions listed as affected under the Software Versions and Fixes section are vulnerable to attack. This includes 11.3AA, 11.3DB, and all 12.0 versions, up to the repaired releases listed in the table. No particular configuration is needed to make a Cisco IOS device vulnerable.

It is possible to filter out the attack traffic using access lists; see the Workarounds section in this document. However, except at Internet firewalls, the appropriate filters are not common in customer configurations. You should carefully evaluate your configuration before assuming that any filtering you have already configured protects you against this attack.

It is impossible to list all Cisco products in this notice; the lists below include only the most commonly used or most asked-about products.

If you are unsure whether your device is running classic Cisco IOS software, log into the device and issue the command **show version**. Classic Cisco IOS software will identify itself simply as "IOS" or "Internetwork Operating System Software". Other Cisco devices either will not have the **show version** command, or will give different output.

Cisco devices that run classic Cisco IOS software include the following:

- Cisco routers in the AGS/MGS/CGS/AGS+, IGS, RSM, 8xx,ubr9xx, 1xxx, 25xx, 26xx, 30xx, 36xx, 38xx, 40xx, 45xx, 47xx, AS52xx, AS53xx, AS58xx, 64xx, 70xx, 72xx (including theubr72xx), 75xx, and 12xxx series.
- Most recent versions of the LS1010 ATM switch.
- Some versions of the Catalyst 2900XL LAN switch.
- The Cisco DistributedDirector.

The affected software versions are relatively new, and are not necessarily available on every device listed above.

## Products Confirmed Not Vulnerable

If you are not running classic Cisco IOS software, then you are *not* affected by this vulnerability. Cisco devices which do *not* run classic Cisco IOS software, and are *not* affected by this vulnerability, include the following:

- 7xx dialup routers (750, 760, and 770 series) are *not* affected.
- Catalyst 19xx, 28xx, 29xx, 3xxx, and 5xxx LAN switches are not affected, except for some versions of the Catalyst 2900XL. However, optional router modules running Cisco IOS software in switch backplanes, such as the RSM module for the Catalyst 5000 and 5500, *are* affected.
- WAN switching products in the IGX and BPX lines are *not* affected.
- The MGX (formerly known as the AXIS shelf) is *not* affected.
- *No* host-based software is affected.
- The Cisco PIX Firewall is *not* affected.
- The Cisco LocalDirector is *not* affected.
- The Cisco Cache Engine is *not* affected.

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

## Details

This vulnerability has Cisco bug ID [CSCdk77426](#). If you are a [registered CCO user](#) and you have logged in, you can view bug details.

## Impact

Attackers can cause Cisco IOS devices to crash and reload. Furthermore, an attacker can repeat the process at will. By striking continuously, an attacker might be able to completely disable a Cisco IOS device until that device was reconfigured by its administrator.

Some Cisco IOS devices have been observed to hang instead of crashing when attacked. These devices do not recover until manually restarted by reset or power cycle. This means that it might be necessary for an administrator to physically visit an attacked device in order to recover from the attack, even if the attacker is no longer actively sending any traffic.

Some devices have crashed without providing stack traces; devices crashed using this vulnerability may indicate that they were "restarted by power-on", even when that is not actually the case.

## Software Versions and Fixes

Many Cisco software images have been or will be specially reissued to correct this vulnerability. For example, regular released version 12.0(2) is vulnerable, as are interim versions 12.0(2.1) through 12.0(2.3). The first fixed interim version of 12.0 mainline software is 12.0(2.4). However, a special release, 12.0(2a), contains *only* the fix for this vulnerability, and does not include any of the other bug fixes from later 12.0 interim releases.

If you were running 12.0(2), and wanted to upgrade to fix this problem, without taking the risk of instability presented by installing the 12.0(2.4) interim release, you could upgrade to 12.0(2a). 12.0(2a) represents a "code branch" from the 12.0(2) base, which merges back into the 12.0 mainline at 12.0(2.4).

In every case, these special releases are one-time spot fixes, and will not be maintained. The upgrade path from, say, 12.0(2a), is to 12.0(3).

See the following table for information about affected and repaired software versions. **All dates in the table are tentative and subject to change.**

Cisco IOS Major Release	Description	Special one-time spot fix release; most stable immediate upgrade path (see above)	First fixed interim release** (fix will carry forward into all later versions)	First fixed regular maintenance release (or other long term upgrade path)
Unaffected releases				
11.2 and earlier, all variants	Unaffected early releases (no syslog server)	Unaffected	Unaffected	Unaffected
11.3, 11.3T, 11.3DA,	11.3 releases without	Unaffected	Unaffected	Unaffected

11.3MA, 11.3NA, 11.3WA, 11.3(2)XA	syslog servers			
11.3-based releases				
11.3AA	11.3 early deployment for AS58xx	11.3(7)AA2, 8-JAN-1999*	11.3(7.2)AA	11.3(8)AA, 15-FEB-1999*
11.3DB	11.3 for Cisco NRP routing blade in Cisco 6400 xDSL DSLAM	–	–	11.3(7)DB2, 18-JAN-1999*
12.0-based releases				
12.0	12.0 mainline	12.0(2a), 8-JAN-1999*	12.0(2.4)	12.0(3), 1-FEB-1999*
12.0T	12.0 new technology early deployment	12.0(2a)T1, 11-JAN-1999*	12.0(2.4)T	12.0(3)T, 15-FEB-1999*
12.0S	ISP support: 7200, RSP, GSR	–	12.0(2.3)S 27-DEC-1998	12.0(2)S***, 18-JAN-1999*
12.0DB	12.0 for Cisco 6400 universal access concentrator node switch processor (lab use)	–	–	12.0(2)DB, 18-JAN-1999*
12.0(1)W	12.0 for Catalyst 8500 and LS1010	12.0(1)W5(5a) and 12.0(1a)W5(5b) (LS1010 platform only)	12.0(1)W5(5.15)	12.0(1)W5(6) (platform support for Catalyst 8540M will be in 12.0(1)W5(7))
12.0(0.6)W5	One-time early deployment for CH-OC12 module in Catalyst 8500 series switches	Unaffected; one-time release	Unaffected	Unaffected; general upgrade path is via 12.0(1)W5
12.0(1)XA3	Short-life release;	Obsolete	Merged	Upgrade to 12.0(2a)T1 and/or

	merged to 12.0T at 12.0(2)T			to 12.0(3)T
12.0(1)XB	Short-life release for Cisco 800 series; merged to 12.0T at 12.0(3)T	12.0(1)XB1	Merged	Upgrade to 12.0(3)T
12.0(2)XC	Short-life release for new features in Cisco 2600, Cisco 3600,ubr7200,ubr900 series; merged to 12.0T at 12.0(3)T	12.0(2)XC1, 7-JAN-1999*	Merged	Upgrade to 12.0(3)T
12.0(2)XD	Short-life release for ISDN voice features; merged to 12.0T at 12.0(3)T.	12.0(2)XD1, 18-JAN-1999*	Merged	Upgrade to 12.0(3)T
12.0(1)XE	Short-life release	12.0(2)XE, 18-JAN-1999*	Merged	Upgrade to 12.0(3)T

**\*All projected dates are estimates, and are subject to change**

\*\* Interim releases are subjected to less rigorous testing than regular maintenance releases, and may have serious bugs.

\*\*\* The vulnerability is fixed in 12.0(2)S. The 12.0(2.3)S interim release is available to the field before the 12.0(2)S regular release because of internal process considerations. This entry is not a misprint.

## Workarounds

You can work around this vulnerability by preventing any affected Cisco IOS device from receiving or processing UDP datagrams addressed to its port 514. This can be done either using packet filtering on surrounding devices, or by using input access list filtering on the affected IOS device itself.

If you use an input access list, that list should be applied to all interfaces to which attackers may be able to send datagrams. This includes not only physical LAN and WAN interfaces, but virtual subinterfaces of those physical interfaces, as well as virtual interfaces and/or interface templates corresponding to GRE, L2TP, L2F, and other tunnelling protocols.

The input access list must block traffic destined for UDP port 514 at any of the Cisco IOS device's own IP addresses, as well as at any broadcast or multicast addresses on which the Cisco IOS device may be listening. It's important to remember to block old-style "all-zeroes" broadcasts as well as new-style "all-ones" broadcasts. It is *not* necessary to block traffic being forwarded to other hosts; only traffic actually addressed to the Cisco IOS device is of interest.

There is no single input access list that will work in all configurations. It is very important that you understand the effect of your access list in your specific configuration before you activate the list.

The following example shows a possible access list for a three-interface router, along with the configuration commands needed to apply that access list. The example assumes that there is no need for input filtering other than as a workaround for this vulnerability.

```
! Deny all multicasts, and all unspecified-net broadcasts, to port 514
access-list 101 deny udp any 224.0.0.0 31.255.255.255 eq 514
! Deny old-style unspecified-net broadcasts
access-list 101 deny udp any host 0.0.0.0 eq 514
! Deny network-specific broadcasts. This example assumes that all of
! the local interfaces are on the class B network 172.16.0.0, subnetted
! everywhere with mask 255.255.255.0. This will differ from network
! to network. Note that we block both new-style and old-style broadcasts.
access-list 101 deny udp any 172.16.0.255 0.0.255.0 eq 514
access-list 101 deny udp any 172.16.0.0 0.0.255.0 eq 514
! Deny packets sent to the addresses of our own network interfaces.
access-list 101 deny udp any host 172.16.1.1 eq 514
access-list 101 deny udp any host 172.16.2.1 eq 514
access-list 101 deny udp any host 172.16.3.3 eq 514
! Permit all other traffic (default would be to deny)
access-list 101 permit ip any any

! Apply the access list to the input side of each interface
interface ethernet 0
ip address 172.16.1.1 255.255.255.0
ip access-group 101 in

interface ethernet 2
ip address 172.16.2.1 255.255.255.0
ip access-group 101 in

interface ethernet 3
ip address 172.16.3.3 255.255.255.0
ip access-group 101 in
```

It can be complicated to list all possible addresses, and especially all possible broadcast addresses, to which attack packets might be sent. If you do not expect to need to forward any legitimate syslog traffic received on an interface, you may wish to simply block all syslog traffic arriving on that interface. Remember that this will affect traffic routed through the Cisco IOS device as well as traffic destined to the device; if the IOS device is expected to forward syslog packets, you will have to do the detailed filtering.

Input access lists have an impact on system performance, and should be installed with a degree of caution, especially on systems that are running very near their capacity limits.

## 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](mailto: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

A third party announced this vulnerability on the "bugtraq@netspace.org" electronic mailing list on December 22, 1998. The third party's announcement included sufficient information to allow any computer-literate person with a moderate interest in security to exploit the vulnerability. On that same day, Cisco sent an informal acknowledgement and a description of the workaround both to the "bugtraq" list and to some other Internet discussion forums, as well as to all Cisco customers who had requested security updates by subscribing to the "cust-security-announce@cisco.com" mailing list.

Cisco has seen the information from "bugtraq" reposted on several Worldwide Web sites catering to those interested in computer security.

All of the Worldwide Web sites in question, and all of the discussion forums, including the "bugtraq" mailing list, are open to the public, and many of them are widely read by people interested in computer and network security. Customers should assume that any potential attacker is likely to know that this vulnerability exists, and furthermore is likely to know how to exploit the vulnerability.

This vulnerability can be exploited using tools available to the public on the Internet; an attacker would not need to write any software to exploit the vulnerability. Minimal skill is required. No special equipment is required.

Despite specifically inviting such reports, Cisco has received no actual reports of malicious exploitation of this vulnerability.

## 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 Web server at <http://www.cisco.com/warp/public/707/cisco-sa-19990111-ios-syslog.shtml>. In addition to Worldwide Web posting, the initial version of this notice is being sent to the following e-mail and Usenet news recipients:

- [cust-security-announce@cisco.com](mailto:cust-security-announce@cisco.com)
- [bugtraq@netspace.org](mailto:bugtraq@netspace.org)
- [first-teams@first.org](mailto:first-teams@first.org) (includes CERT/CC)
- [first-info@first.org](mailto:first-info@first.org)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [comp.dcom.sys.cisco](mailto:comp.dcom.sys.cisco)
- [nanog@merit.edu](mailto:nanog@merit.edu)
- Various internal Cisco mailing lists

Future updates of this advisory, if any, will be placed on Cisco's Worldwide Web server, 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 1.1	1999 January 11	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 Web site at [http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html). This includes instructions for press inquiries regarding Cisco security notices.

---

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

---

Updated: Jan 11, 1999

Document ID: 13660

---