

Cisco Security Advisory: Cisco IOS Malformed OSPF Packet Causes Reload

Document ID: 61365

Advisory ID: cisco-sa-20040818-ospf

<http://www.cisco.com/warp/public/707/cisco-sa-20040818-ospf.shtml>

Revision 1.4

Last Updated 2005 March 29 1400 UTC (GMT)

For Public Release 2004 August 18 1500 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 Cisco device running Internetwork Operating System (IOS) ® and enabled for the Open Shortest Path First (OSPF) protocol is vulnerable to a Denial of Service (DoS) attack from a malformed OSPF packet. The OSPF protocol is not enabled by default.

The vulnerability is only present in Cisco IOS release trains based on 12.0S, 12.2, and 12.3. Releases based on 12.0, 12.1 mainlines, and all Cisco IOS images prior to 12.0 are not affected.

Cisco has made free software available to address this vulnerability.

There are workarounds available to mitigate the effects.

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20040818-ospf.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

This vulnerability was introduced by a code change that was committed to the 12.0S, 12.2, and 12.3 based release trains, causing these trains to be vulnerable. All Cisco devices running a vulnerable release train and running OSPF process are vulnerable.

Some release trains that are not vulnerable are explicitly listed below for clarification. The release trains that are not mentioned below are not vulnerable.

Release Train	Vulnerable Versions
10.x based releases	Not vulnerable
11.x based releases	Not vulnerable
12.0 based releases (except for 12.0.S based releases)	Not vulnerable
12.1 based releases	Not vulnerable
12.0.S	12.0(22)S and later
12.0.SX	12.0(23)SX and later
12.0.SY	12.0(22)SY and later
12.0.SZ	12.0(23)SZ and later
12.2 mainline	Not vulnerable
12.2.B	12.2(15)B and later
12.2.BC	12.2(15)BC and later
12.2.BX	12.2(15)BX and later
12.2.BZ	12.2(15)BZ and later
12.2.CX	12.2(15)CX and later
12.2.EW	12.2(18)EW and later
12.2.MC	12.2(15)MC1 and later
12.2.S	12.2(18)S and later
12.2.SE	12.2(18)SE and later
12.2.SV	12.2(18)SV and later
12.2.SW	12.2(18)SW and later
12.2.SZ	12.2(14)SZ and later
12.2.T	12.2(15)T and later

12.2.YU	12.2(11)YU and later
12.2.YV	12.2(11)YV and later
12.2.ZD	12.2(13)ZD and later
12.2.ZE	12.2(13)ZE and later
12.2.ZF	12.2(13)ZF and later
12.2.ZG	12.2(13)ZG and later
12.2.ZH	12.2(13)ZH and later
12.2.ZJ	12.2(15)ZJ and later
12.2.ZK	12.2(15)ZK and later
12.2.ZL	12.2(15)ZL and later
12.2.ZN	12.2(15)ZN and later
12.2.ZO	12.2(15)ZO and later
12.3	All 12.3 releases
12.3.B	All 12.3.B releases
12.3.BW	All 12.3.BW releases
12.3.T	All 12.3.T releases
12.3.XA	All 12.3.XA releases
12.3.XB	All 12.3.XB releases
12.3.XC	All 12.3.XC releases
12.3.XE	All 12.3.XE releases

A Cisco device which is running an OSPF process will have a line in the configuration defining the process number, which can be seen by issuing the **command show running-config**:

```
router ospf {process number}
```

To determine the software running on a Cisco product, log in to the device and issue the **show version** command to display the system banner. Cisco IOS software will identify itself as "Internetwork Operating System Software" or simply "IOS." On the next line of output, the image name will be displayed between parentheses, followed by "Version" and the Cisco IOS release name. Other Cisco devices will not have the **show version** command, or will give different output.

The following example identifies a Cisco product running Cisco IOS release 12.0(3) with an installed image name of C2500-IS-L:

```
Cisco Internetwork Operating System Software IOS (TM)
2500 Software (C2500-IS-L), Version 12.0(3), RELEASE SOFTWARE
```

The release train label is "12.0." The next example shows a product running Cisco IOS release 12.0(2a)T1 with an image name of C2600-JS-MZ:

```
Cisco Internetwork Operating System Software IOS (tm)
C2600 Software (C2600-JS-MZ), Version 12.0(2a)T1, RELEASE SOFTWARE (fc1)
```

Additional information about Cisco IOS release naming can be found at <http://www.cisco.com/warp/public/620/1.html>.

Products Confirmed Not Vulnerable

These products are confirmed not vulnerable:

- Products that are not running Cisco IOS are not affected.
- Products running Cisco IOS versions 12.0 and earlier (excluding 12.0 S), 12.1 mainline and 12.2 mainline are not vulnerable.
- Products running IOS release trains that are not mentioned in the above table are not vulnerable.
- Products running any version of Cisco IOS that do **not** have OSPF configured are not vulnerable.

Details

OSPF is a routing protocol defined by RFC 2328. It is designed to manage IP routing inside an Autonomous System (AS). OSPF packets use IP protocol number 89.

A vulnerability exists in the processing of an OSPF packet that can be exploited to cause the reload of a system.

Since OSPF needs to process unicast packets as well as multicast packets, this vulnerability can be exploited remotely. It is also possible for an attacker to target multiple systems on the local segment at a time.

Using OSPF Authentication as described in the workarounds section can be used to mitigate the effects of this vulnerability. Using OSPF Authentication is a highly recommended security best practice

A Cisco device receiving a malformed OSPF packet will reset and may take several minutes to become fully functional. This vulnerability may be exploited repeatedly resulting in an extended DOS attack. This issue is documented in bug ID CSCec16481.

Impact

Successful exploitation of this vulnerability results in a reload of the device. Repeated exploitation could result in a sustained DoS attack.

Software Versions and Fixes

Each row of the table describes a release train and the platforms or products for which it is intended. If a given release train is vulnerable, then the earliest possible releases that contain the fix and the anticipated date of availability for each are listed in the Rebuild, Interim, and Maintenance columns. In some cases, no rebuild of a particular release is planned; this is marked with the label "Not scheduled." A device running any release in the given train that is earlier than the release in a specific column (less than the earliest fixed release) is known to be vulnerable, and it should be upgraded at least to the indicated release or a later version (greater than the

earliest fixed release label).

When selecting a release, keep in mind the following definitions:

- **Maintenance** Most heavily tested and highly recommended release of any label in a given row of the table.
- **Rebuild** Constructed from the previous maintenance or major release in the same train, it contains the fix for a specific vulnerability. Although it receives less testing, it contains only the minimal changes necessary to effect the repair. Cisco has made available several rebuilds of mainline trains to address this vulnerability, but strongly recommends running only the latest maintenance release on mainline trains.
- **Interim** Built at regular intervals between maintenance releases and receives less testing. Interims should be selected only if there is no other suitable release that addresses the vulnerability, and interim images should be upgraded to the next available maintenance release as soon as possible. Interim releases are not available through manufacturing, and usually they are not available for customer download from CCO without prior arrangement with the Cisco Technical Assistance Center (TAC).

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 TAC for assistance, as shown in the section following this table.

Major Release	Availability of Repaired Releases		
Affected 12.0–Based Release	Rebuild	Interim	Maintenance
12.0(22)S and later	12.0(22)S6		
	12.0(23)S5		
	12.0(24)S2c		
	12.0(24)S4		
	12.0(25)S1d		
	12.0(25)S2		
	12.0(26)S1		12.0(27)S
12.0(23)SX and later	12.0(25)SX2		
12.0(22)SY and later	Migrate to		
12.0(23)SZ and later	12.0(23)S5 or later		12.0(27)SZ
Affected 12.2–Based Release	Rebuild	Interim	Maintenance
12.2(15)B and	Migrate to		

later	12.3(4)T or later		
12.2(15)BC and later	12.2(15)BC1c		
	12.2(15)BC2		
12.2(15)BX and later	Migrate to		
12.2(15)BZ and later	12.3(7)XI1 or later		
	Migrate to		
12.2(15)CX and later	12.3(7)XI1 or later		
	Migrate to 12.2(15)BC2 or later		
12.2(18)EW	12.2(18)EW1		12.2(20)EW
12.2(15)MC1 and later	12.2(15)MC2a available upon request		
12.2(18)S and later	12.2(20)S		
	12.2(18)S5		
12.2(18)SE and later			12.2(20)SE
12.2(18)SV and later			12.2(22)SV
12.2(18)SW and later			12.2(20)SW
12.2(14)SZ and later	Migrate to		
12.2(15)T and later	12.2(20)S4 or later		
	12.2(15)T8		
12.2(11)YU and later	Migrate to		
12.2(11)YV and later	12.3(4)T or later		
	Migrate to		
12.2(13)ZD and later	12.3(4)T or later		
	Migrate to 12.3T		
12.2(13)ZE and later	or later		
	Migrate to 12.3 or later		
12.2(13)ZF and later	later		
	Migrate to		
12.2(13)ZG and later	12.3(4)T or later		
	Migrate to		
12.2(13)ZH and later	12.3(4)T or later		
	Migrate to		
12.2(15)ZJ and later	12.3(4)T or later		
	Migrate to 12.3T or later		

12.2(15)ZK and later	12.2(15)ZK2		
12.2(15)ZL and later	Migrate to		
12.2(15)ZN and later	12.3(7)T or later Migrate to		
12.2(15)ZO and later	12.3(2)T4 or later Migrate to		
Affected 12.3–Based Release	12.2(15)T8 or later Rebuild	Interim	Maintenance
12.3	12.3(3f)		12.3(5)
12.3B	12.3(5a)B		
12.3BW	Migrate to 12.3B or later		
12.3T	12.3(2)T4		12.3(4)T
12.3XA	Migrate to 12.3(7)T or later		
12.3XB	12.3(2)XB3		
12.3XC	Migrate to 12.3(8)T or later		
12.3XE	Migrate to 12.3(8)T or later		

Workarounds

The effectiveness of any workaround 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 is the most appropriate for use in the intended network before it is deployed.

There are multiple workarounds available to mitigate the effects of this vulnerability.

Using OSPF Authentication

OSPF authentication may be used as a workaround. OSPF packets without a valid key will not be processed. MD5 authentication is highly recommended, due to inherent weaknesses in plain text authentication. With plain text authentication, the authentication key will be sent unencrypted over the network, which can allow an attacker on a local network segment to capture the key by sniffing packets.

Refer to <http://www.cisco.com/warp/public/104/25.shtml> for more information about OSPF authentication.

Infrastructure Access Control Lists

Although it is often difficult to block traffic transiting your network, it is possible to identify traffic which should never be allowed to target your infrastructure devices and block that traffic at the border of your network. Infrastructure ACLs are considered a network security best practice and should be considered as a

long-term addition to good network security as well as a workaround for this specific vulnerability. The white paper "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for infrastructure protection ACLs:
<http://www.cisco.com/warp/public/707/iacl.html>.

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/en/US/docs/general/warranty/English/EU1KEN.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/en/US/support/tsd_cisco_worldwide_contacts.html 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

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerability described in this advisory.

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-20040818-ospf.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
- first-teams@first.org (includes CERT/CC)
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.netsys.com
- comp.dcom.sys.cisco@newsgate.cisco.com

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 1.4	2005-March-29	In the Software Versions and Fixes section under "Affected 12.2-Based Release" for "12.2(15)BX and later, changed the rebuild cell "12.2(16)BX Migrate to 12.3(7)XI1 or later" to "Migrate to 12.3(7)XI1 or later."
	2004-August-27	

Revision 1.3		Removed the sentences "Several parameters need to be known by an attacker to successfully exploit this vulnerability. These are the OSPF area number, netmask, hello, and dead timers that are configured on the targeted interface." from the Details section.
Revision 1.2	2004–August–21	In the IOS fixed software table, for the row "12.2(18)S and later," moved 12.2(20)S from Maintenance column to Rebuild column.
Revision 1.1	2004–August–20	Added text above the table in the Software Versions and Fixes section. In the IOS fixed software table, for the row "12.2(18)EW," added 12.2(20)EW to the Maintenance column. In the IOS fixed software tables, removed "*" and "**" removed from the table headings.
Revision 1.0	2004–August–18	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>.

[Contacts & Feedback](#) | [Help](#) | [Site Map](#) © 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Mar 29, 2005

Document ID: 61365
