

Cisco Security Advisory: Cisco IOS ARP Table Overwrite Vulnerability

Document ID: 13600

Advisory ID: cisco-sa-20011115-ios-arp-overwrite

<http://www.cisco.com/warp/public/707/cisco-sa-20011115-ios-arp-overwrite.s>

Revision 1.3

Last Updated 2002 July 22 1700 UTC (GMT)

For Public Release 2001 November 15 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

It is possible to send an Address Resolution Protocol (ARP) packet on a local broadcast interface (for example, Ethernet, cable, Token Ring, FDDI) which could cause a router or switch running specific versions of Cisco IOS® Software Release to stop sending and receiving ARP packets on the local router interface. This will in a short time cause the router and local hosts to be unable to send packets to each other. ARP packets received by the router for the router's own interface address but a different Media Access Control (MAC) address will overwrite the router's MAC address in the ARP table with the one from the received ARP packet. This was demonstrated to attendees of the Black Hat conference and should be considered to be public knowledge. This attack is only successful against devices on the segment local to the attacker or attacking host.

This vulnerability is documented in Cisco Bug ID CSCdu81936, and a workaround is available.

The complete notice will be available at

<http://www.cisco.com/warp/public/707/cisco-sa-20011115-ios-arp-overwrite.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

The following products are affected if they run a software release that has the defect.

To determine if a Cisco product is running an affected IOS, log in to the device and issue the command **show version**. Cisco IOS software will identify itself as "**Internetwork Operating System Software**" or "**IOS (tm)**" software and will display a version number. Other Cisco devices either will not have the command show version, or will give different output. Compare the version number obtained from the router with the versions presented in the Software Versions and Fixes section below.

Cisco devices that may be running with affected IOS software releases include:

- Cisco routers in the AGS/MGS/CGS/AGS+, IGS, RSM, 800,ubr900, 1000, 1400, 1500, 1600, 1700, 2500, 2600, 3000, 3600, 3800, 4000, 4500, 4700, AS5200, AS5300, AS5800, 6400, 7000, 7200, ubr7200, 7500, and 12000 series
- Most recent versions of the LS1010 ATM switch
- Catalyst 2900XL and 3500XL LAN switches
- Catalyst 2950 LAN switch
- Catalyst 3550 switch
- Catalyst 2948G-L3 & 4908G-L3
- Catalyst 4000 Layer 3 services module (WS-X4232-L3)
- Catalyst 5000 RSM/RSFC
- Catalyst 6000 MSFC
- Catalyst 6000 running native IOS
- Catalyst 8500 MSR/CSR
- Cisco DistributedDirector

Products Confirmed Not Vulnerable

If you are not running Cisco IOS software, you are not affected by this vulnerability.

Cisco products that do not run Cisco IOS software and are not affected by this defect include, but are not limited to:

- 700 series dialup routers (750, 760, and 770 series) are not 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.
- The Catalyst 2901/2902, 2948G, 2980G, 4000, 5000, and 6000 switches running CatOS.

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

Details

ARP packets, both request and reply, received by the router for the router's own interface address or global Network Address Translation (NAT) entries, but with a different MAC address, will overwrite the router's MAC address in the router's ARP table with the one in the ARP request or reply. Cisco IOS router devices will defend the MAC address of an interface for several attempts, but in an attempt to prevent an ARP storm, the device will accept the incorrect information into the ARP table, which causes the interface to stop accepting new ARP entries, and entries will not be accepted or updated in the ARP table. This behavior has been repaired to properly defend the interface MAC address, with rate limiting the response to avoid an ARP storm on the local network. This attack can only be carried out from the local network. This defect also impacts HSRP virtual interfaces. This defect is documented in Cisco Bug ID CSCdu81936 and is repaired in future versions of Cisco IOS code. This defect is duplicated by the following Cisco Bug ID's: CSCdv83509, CSCdv63206, CSCdv77242, CSCdv77220, CSCdu85209. Additionally, a configuration workaround is available.

Impact

This issue can cause a Cisco Router to be vulnerable to a Denial-of-Service attack, once the ARP table entries time out. This defect does not result in a failure of confidentiality of information stored on the unit, nor does this defect allow hostile code to be loaded onto a Cisco device. This defect may cause a Denial-of-Service on the management functions of a Cisco Layer 2 Switch, but does not affect traffic through the device.

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. 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 defect. Although it receives less testing, it contains only the minimal changes necessary to effect the repair.

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 via 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 following section.

More information on Cisco IOS software release names and abbreviations is available at <http://www.cisco.com/warp/public/620/1.html>.

Major Release	Description or Platform Affected Earlier Releases	Availability of Repaired Releases*		
		Rebuild	Interim**	Maintenance
11.1 and earlier, all variants	Numerous	Upgrade to repaired release or use workaround		
11.2–based Releases		Rebuild	Interim**	Maintenance
11.2	Major release for all platforms	Not affected after 11.2(13)		
11.2P	New platform support	Not affected after 11.2(12)P		
11.3–based Releases		Rebuild	Interim**	Maintenance
11.3	Major release for all platforms	Not affected after 11.3(3)		
11.3T	Early deployment major release, feature–rich for early adopters	Not affected after 11.3(3)		
12.0–based Releases		Rebuild	Interim**	Maintenance
12.0	General Deployment (GD) candidate: all platforms		12.0(19.6)	
12.0DA	xDSL support: 6100, 6200	Unavailable Upgrade recommended to 12.2DA		
12.0DB	Early deployment release for 6400 NSP	Unavailable		
12.0DC	Early deployment release for 6400 NRP	Upgrade recommended to 12.1T or later Unavailable Upgrade recommended to 12.2(2)B when available		
12.0S	Core/ISP support: GSR, RSP, c7200	available		12.0(21)S 2002–Jan–14
12.0SC	Cable/broadband ISP:ubr7200	Unavailable		

		Upgrade recommended to 12.1EC, or use workaround		
12.0SL	10000 ESR: c10k	Unavailable		
		Upgrade recommended to 12.0ST, or use workaround		
12.0SP	c10720			12.0(20)SP
		To Be Announced		
12.0ST	MPLS/Tag Switching, GSR 12000, 7200, 7500			12.0(20)ST 2001–Nov–26
12.0T	Early Deployment(ED): VPN, Distributed Director, various platforms	Unavailable		
12.0W5	Catalyst switches: cat8510c, cat8540c, ls1010, cat8510m, cat8540m, cat5atm	Upgrade recommended to 12.1(11)		12.0(20)W5(24)
	Catalyst switches: cat2948g–L3, cat4232			2002–Jan–07 12.0(18)W5(22a)
	Catalyst switches: c6msm			2001–Dec–1 12.0(16)W5(21b)
				2001–Nov–29
12.0WC	Catalyst 2900xl	12.0(5)WC3 2002–Jan		
12.0WT	Catalyst switches: cat4840g	Not affected		
12.0XA	Early Deployment (ED): limited platforms	Unavailable		
12.0XB	Short–lived early deployment release	Upgrade recommended to 12.1(11)		
		Unavailable		
12.0XC	Early Deployment (ED): limited platforms	Upgrade recommended to 12.1(11)		
		Unavailable		
12.0XD	Early Deployment (ED): limited platforms	Upgrade recommended to 12.1(11)		
		Unavailable		
12.0XE		Upgrade recommended to 12.1(11)		
		Unavailable		

	Early Deployment (ED): limited platforms	Upgrade recommended to 12.1(11)E, available 2001–Dec–10
12.0XF	Early Deployment (ED): limited platforms	Unavailable
12.0XG	Early Deployment (ED): limited platforms	Upgrade recommended to 12.1(11) Unavailable
12.0XH	Early Deployment (ED): limited platforms	Upgrade recommended to 12.1(11) Unavailable
12.0XI	Early Deployment (ED): limited platforms	Upgrade recommended to 12.1(11) Unavailable
12.0XJ	Early Deployment (ED): limited platforms	Upgrade recommended to 12.1(11) Unavailable
12.0XK	Early Deployment (ED): limited platforms	Upgrade recommended to 12.1(11) Unavailable
12.0XL	Early Deployment (ED): limited platforms	Upgrade recommended to 12.1(11) Unavailable
12.0XM	Short-lived early deployment release	Upgrade recommended to 12.1(11) Unavailable
12.0XN	Early Deployment (ED): limited platforms	Upgrade recommended to 12.1(11) Unavailable
12.0XP	Early Deployment (ED): limited platforms	Upgrade recommended to 12.1(11) Unavailable
12.0XQ	Short-lived early deployment release	Workaround recommended Unavailable
12.0XR	Short-lived early deployment release	Upgrade recommended to 12.1(11) Unavailable
12.0XS	Short-lived early deployment release	Upgrade recommended to 12.1(11) Unavailable Upgrade recommended to 12.1(11)E, available
12.0XU	Early Deployment (ED): limited platforms	2001–DEC–10 Unavailable

Upgrade recommended or use workaround

12.0XV	Short-lived early deployment release	Unavailable			
12.1-based Releases		Upgrade recommended to 12.2	Rebuild	Interim**	Maintenance
12.1	General Deployment (GD) candidate: all platforms		12.1(10.3)	12.1(11)	
12.1AA	Dial Support			12.1(10)AA	2001-Nov-12
12.1DA	xDSL Support: 6100, 6200	Unavailable			
		Upgrade recommended to 12.2.T			
12.1DB	Cisco 6400 Universal Access Concentrator	Upgrade recommended to 12.2(2)B when available			
12.1DC	xDSL NRP support: c6400r	Upgrade recommended to 12.2(2)B when available			
12.1E	Core/ISP Support: GSR, RSP, c7200			12.1(11)E	
	Catalyst 6000			2001-DEC-10	12.1(08a)E05
12.1EA	Catalyst 2950	12.1(6)EA2			
	Catalyst 3550	12.1(6)EA1a			
12.1EC	Early Deployment (ED): ubr7200, UBR Headend platforms		12.1(8.5)EC	12.1(9)EC	
12.1EX	Catalyst 6000	Unavailable			
		Upgrade recommended to 12.1(11)E			
12.1EY	Catalyst 8510, 8540, LS1010	Not Affected			
12.1EZ	Early Deployment (ED): limited platforms	12.1(6)EZ4			
		2001-Nov-02			
12.1T	New technology Early Deployment (ED): all platforms	Unavailable			
		Upgrade recommended to 12.2			
12.1XA	Early Deployment (ED): limited platforms	Unavailable			
		Upgrade recommended to 12.2			
12.1XB		Unavailable			

	Early Deployment (ED): limited platforms	Upgrade recommended to 12.2		
12.1XC	Early Deployment (ED): limited platforms	Unavailable		
12.1XD	Early Deployment (ED): limited platforms	Upgrade recommended to 12.2 Unavailable		
12.1XE	Early Deployment (ED): limited platforms	Upgrade recommended to 12.2 Unavailable		
12.1XF	Early Deployment (ED): limited platforms	Upgrade recommended to 12.2		
		12.1(2)XF5		
		2002–Jan		
12.1XG	Early Deployment (ED): limited platforms	12.1(3)XG6		
		2002–Jan		
12.1XH	Early Deployment (ED): limited platforms	Unavailable		
12.1XI	Early Deployment (ED): limited platforms	Upgrade recommended to 12.2 Unavailable		
12.1XJ	Early Deployment (ED): limited platforms	Upgrade recommended to 12.2 Unavailable		
12.1XK	Early Deployment (ED): limited platforms	Upgrade recommended to 12.2 Unavailable		
12.1XL	Early Deployment (ED): limited platforms	Upgrade recommended to 12.2 Unavailable		
12.1XM	Early Deployment (ED): limited platforms	Upgrade recommended to 12.2		
		12.1(5)XM6		
		2001–Dec–03		
12.1XP	Early Deployment (ED): limited platforms	Unavailable		
12.1XQ	Early Deployment (ED): limited platforms	Upgrade recommended to 12.2(2)T Unavailable		
12.1XR	Early Deployment (ED): limited platforms	Upgrade recommended to 12.2(2)T Unavailable		

Upgrade recommended to 12.2(7)T

12.1XS	Early Deployment (ED): limited platforms	12.2(2)XC1 2001-DEC-3		
12.1XT	Early Deployment (ED): limited platforms	Unavailable		
12.1XU	Early Deployment (ED): limited platforms	Upgrade recommended to 12.2(7)T Not affected		
12.1XV	Early Deployment (ED): limited platforms	12.2(2)XB2 2001-DEC-17		12.2(2)XB2 2001-DEC-17
12.1XW	Early Deployment (ED): limited platforms			12.1(11)
12.1XX	Early Deployment (ED): limited platforms			12.1(11)
12.1YA	Early Deployment (ED): limited platforms			12.2(2)XB
12.1YB	Early Deployment (ED): limited platforms	12.1(5)YB5 2002-Jan		
12.1YC	Early Deployment (ED): limited platforms	12.1(5)YC2 2002-Jan		
12.1YD	Early Deployment (ED): limited platforms	Migrate to 12.2(7)T		
12.1YE	Early Deployment (ED): limited platforms	12.1(5)YE4 2001-Nov-19		
12.1YF	Early Deployment (ED): limited platforms	12.1(5)YF3 2001-Nov		
12.1YH	Early Deployment (ED): limited platforms	Not Affected		
Affected 12.2-based Releases		Rebuild	Interim**	Maintenance
12.2	General Deployment (GD) candidate: all platforms		12.2(4.2)	12.2(5)

12.2DD	7200, 7400	12.2(2)DD1 2001–Nov–19		
12.2T	Early Deployment (ED): limited platforms			12.2(7)T 2002–Feb
12.2XA	Early Deployment (ED): limited platforms	12.2(2)XA4 2001–Dec–3		
12.2XB	Early Deployment (ED): limited platforms	12.2(2)XB2 2001–Dec–17		
12.2XC	Early Deployment (ED): limited platforms	12.2(2)XC1 2001–DEC–3		
12.2XD	Early Deployment (ED): limited platforms	12.2(1)XD3 2002–Jan		
12.2XE	Early Deployment (ED): limited platforms	12.2(1)XE2 2002–Jan		
12.2XG	Early Deployment (ED): limited platforms	12.2(2)XG1 2001–DEC–17		
12.2XH	Early Deployment (ED): limited platforms	12.2(2)XH2 2002–Jan		
12.2XI	Early Deployment (ED): limited platforms			
12.2XJ	Early Deployment (ED): limited platforms	12.2(2)XJ2 2002–Jan		
12.2XK	Early Deployment (ED): limited platforms	12.2(2)XK5 2002–Jan		
12.2XQ	Early Deployment (ED): limited platforms	12.2(2)XQ2 2002–Jan		
Notes				
* All dates are estimated and subject to change.				
** Interim releases are subjected to less rigorous testing than regular maintenance releases, and may have serious bugs.				

*** This release does not have a rebuild solution. Customers should upgrade to 12.2T when it becomes available. This is not a misprint.

Workarounds

The workaround for this vulnerability is to enter the router interface MAC address into the arp table with a configuration entry, sometimes known as "hard coding" the ARP table entry.

The syntax for this command for routers and switches running IOS is as follows:

```
arp <ip-address> <hardware-address> <type>
```

The caveat to this workaround is identified with defect CSCdv04366, which will clear all manually entered MAC addresses from the ARP table, when they are the same as the interface MAC address, when the command "clear arp" is issued on the router. This workaround does not survive a reboot of the router, and must be re-written to the configuration after any reload or reboot.

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

This vulnerability was disclosed at the Black Hat conferences in Las Vegas this year by Kevin DePeugh <v0nelm0@best.com> and Jeff Nathan <jeff@wwti.com>. There have been isolated reports of exploitation of this vulnerability, and workarounds implemented circumvented the attacks. This attack is known as the "Sonic Boom," and tools are readily available.

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 notice will be posted on Cisco's Worldwide Web site at <http://www.cisco.com/warp/public/707/cisco-sa-20011115-ios-arp-overwrite.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
- first-teams@first.org (includes CERT/CC)
- cisco@spot.colorado.edu
- comp.dcom.sys.cisco
- firewalls@lists.gnac.com
- Various internal Cisco mailing lists

Future updates of this notice, 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 URL given above for any updates.

Revision History

Revision 1.3	2002–July–22	Updates to Software Versions and Fixes section.
Revision 1.2	2001–December–18	Updates to Summary, Affected Products, Impact, Software Versions and Fixes, and Workaround sections.
Revision 1.1	2001–November–21	Release table updates
Revision 1.0	2001–November–15	For public release 15–NOV–2001 08:00 AM US/Pacific (UTC–0700)

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: Jul 22, 2002

Document ID: 13600
