

Cisco Security Advisory: Scanning for SSH Can Cause a Crash

Document ID: 24862

Advisory ID: cisco-sa-20020627-ssh-scan

<http://www.cisco.com/warp/public/707/cisco-sa-20020627-ssh-scan.shtml>

Revision 1.0

For Public Release 2002 June 27 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

While fixing vulnerabilities mentioned in the Cisco Security Advisory: Multiple SSH Vulnerabilities (http://www.cisco.com/en/US/products/products_security_advisory09186a00800b168e.shtml) we inadvertently introduced an instability in some products. When an attacker tries to exploit the vulnerability VU#945216 (described in the CERT/CC Vulnerability Note at <http://www.kb.cert.org/vuls/id/945216>) the SSH module will consume too much of the processor's time, effectively causing a DoS. In some cases the device will reboot. In order to be exposed SSH must be enabled on the device.

Affected product lines are:

- All devices running Cisco IOS® Software supporting SSH. This includes routers and switches running Cisco IOS Software.
- Catalyst 6000 switches running CatOS.
- Cisco PIX Firewall.
- Cisco 11000 Content Service Switch family.

No other Cisco product is vulnerable. It is possible to mitigate this vulnerability by preventing, or having control over, the SSH traffic.

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20020627-ssh-scan.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

These products are vulnerable:

- All devices running Cisco IOS Software supporting SSH. This includes routers and switches running Cisco IOS Software.
- Catalyst 6000 switches running CatOS.
- Cisco PIX Firewall.
- Cisco 11000 Content Service Switch family.

Product Category	Vulnerability ID
IOS	CSCdw33027
PIX	CSCdw29965
VPN 3000	Not affected
Catalyst 6000	CSCdv85279 and CSCdw59394
CSS 11000	CSCdx59197

All software releases listed in the http://www.cisco.com/en/US/products/products_security_advisory09186a00800b168e.shtml (Cisco Security Advisory: Multiple SSH Vulnerabilities), including all subsequent software releases that contain the patches addressed by that advisory are vulnerable.

Products Confirmed Not Vulnerable

All software that does not contain fixes for the issues listed in the previous SSH advisory are not vulnerable to the issue described in this advisory. However, falling back to a previous software release will leave you exposed to the vulnerabilities described in the previous advisory and you will lose any additional features or functionalities introduced in the newer releases.

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

Details

While fixing the vulnerabilities listed in http://www.cisco.com/en/US/products/products_security_advisory09186a00800b168e.shtml (Cisco Security Advisory: Multiple SSH Vulnerabilities) an instability is introduced in some products. When exposed to an overly large packet, the SSH process will consume a large portion of the processor's instruction cycles, effectively causing a DoS. The capability to create such a packet is available in publicly available exploit code. In some cases this availability attack may result in a reboot of the device. In order to be exposed SSH must be enabled on the device.

The vulnerability in question is named CRC-32 Check in the http://www.cisco.com/en/US/products/products_security_advisory09186a00800b168e.shtml. It is also marked as VU#945216 and described in the CERT/CC Vulnerability Note at <http://www.kb.cert.org/vuls/id/945216>.

Impact

By repeatedly exploiting this vulnerability an attacker can cause a denial of service, though Cisco products remain unaffected to the exploits that are trying to exploit vulnerabilities listed in http://www.cisco.com/en/US/products/products_security_advisory09186a00800b168e.shtml.

Software Versions and Fixes

For CSS 11000 family, the vulnerability is fixed in the following software releases.

WebNS	R5.00.045 or later (available now) 5.10.1.01 available July 2002
-------	---------------------------------------------------------------------

For Catalyst 6000 switches, the vulnerability is fixed in the following CatOS releases. This table lists the first fixed release.

CatOS	6.3(3.6), 7.1(0.94), 7.2(0.14)PEN
-------	-----------------------------------

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. 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 following section.

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

For PIX Firewall software, use the following table to determine affected and fixed software releases.

Train	Description of Image or Platform	Availability of Fixed Releases*		
		Rebuild	Interim**	Maintenance
5.x-based Releases				

5.2	General Deployment (GD) for Classic, 10000, 506, 506E, 510, 515, 515E, 520 and 525		5.2(6)202 Available through	5.2(7)
5.3	Early Deployment (ED) for Classic, 10000, 506, 506E, 510, 515, 515E, 520, 525 and 535		TAC 5.3(2)205 Available through	5.3(3)
6.x–based Releases		Rebuild	TAC Interim**	Maintenance
6.0	Early Deployment (ED) for 501, 506, 506E, 515, 515E, 520, 525 and 535		6.0(1)106 Available through	6.0(2)
6.1	Early Deployment (ED) for 501, 506, 506E, 515, 515E, 520, 525 and 535		TAC 6.1(1)105 Available through	6.1(2)
6.2	Early Deployment (ED) for 501, 506, 506E, 515, 515E, 520, 525 and 535		TAC 6.2(0)222 Available through	6.2(1)

TAC

For Cisco IOS software, use the following table to determine affected and fixed software releases. This table always lists the first fixed release, which is not necessarily the recommended release for your particular environment.

Train	Description of Image or Platform	Availability of Fixed Releases*		
12.0–based Releases		Rebuild	Interim**	Maintenance
12.0S	Core/ISP support: GSR, RSP, c7200	12.0(17)S4	12.0(20.4)S	12.0(21)S
12.0SP	Core/ISP support: GSR, RSP, c7200	12.0(20)SP2	12.0(20.4)SP	
12.0ST	Core/ISP support: GSR, RSP, c7200	12.0(17)ST5	12.0(20.3)ST2	12.0(21)S
12.0XB	Early Deployment Release	Not Scheduled		
		Migrate to 12.1(1)T or later		
12.0XM	Early Deployment Release	Not Scheduled		
		Migrate to 12.1(3)T or later		
12.0XV	Early Deployment Release	Not Scheduled		
		Migrate to 12.1(2)T or later		
12.1–based Releases		Rebuild	Interim**	Maintenance

12.1	General deployment release for all platforms	SSH not supported		
12.1E	Core/ISP support: GSR, RSP, c7200, Catalyst 6000	12.1(8b)E8	12.1(10.5)E	12.1(11b)E
12.1EC	Early Deployment Release		12.1(10.5)EC	12.1(12c)EC
12.1(1)EX	Early Deployment Release	Not Scheduled		
		Migrate to 12.1(3)T or later		
12.1(5c)EX	Catalyst 6000 support	Not Scheduled		
		Migrate to 12.1(6)EX or later		
12.1(8a)EX	12.1E based XED	Not Scheduled		
		Migrate to 12.1(11)E or later		
12.1(9)EX	Early Deployment Release	Not Scheduled		
		Migrate to 12.1(10)EX or later		
12.1T	Early Deployment(ED): VPN, Distributed Director, various platforms	Not Scheduled		
12.1XB	Early Deployment Release	Migrate to 12.2 or later		
		Not Scheduled		
12.1XC	Early Deployment (ED): limited platforms	Migrate to 12.1(5)YB or later		
		Not Scheduled		
12.1XF	Early Deployment (ED): 811 and 813 (c800 images)	Migrate to 12.2 or later		Not planned, migrate to 12.1(5)T or later
		12.1(2)XF6 Release date to be determined		
12.1XG	Early Deployment (ED): 800, 805, 820, and 1600	Migrate to 12.2 or later		Not planned, migrate to 12.2(1)T or later
		12.1(3)XG7 Release date to be determined		
12.1XH	Early Deployment (ED): limited platforms	Not Scheduled		
12.1XI	Early Deployment (ED): limited platforms	Migrate to 12.2 or later		
		Not Scheduled		
12.1XJ	Early Deployment (ED): limited	Migrate to 12.2 or later		
		Not Scheduled		
		Migrate to 12.2(2)T or later		

	platforms			
12.1XL	Early Deployment (ED): limited platforms	Not Scheduled		
12.1XM	Short-lived early deployment release	Migrate to 12.2 or later 12.1(5)XM7		Not planned, migrate to 12.2(1)T or later
12.1XP	Short-lived early deployment release	Not Scheduled		
12.1XQ	Short-lived early deployment release	Migrate to 12.2(2)T or later Not Scheduled		
12.1XT	Early Deployment (ED): 1700 series	Migrate to 12.2(2)XB or later Not Scheduled		
12.1XU	Early Deployment (ED): limited platforms	Migrate to 12.2(2)T or later Not Scheduled		
12.1YB	Short-lived early deployment release	Migrate to 12.2T or later 12.1(5)YB6 Release date to be determined		Not planned, migrate to 12.2(2)T or later
12.1YC	Short-lived early deployment release	12.1(5)YC3 Release date to be determined		Not planned, migrate to 12.2(4)T or later
12.1YD	Short-lived early deployment release	Not Scheduled		
12.1YE	Short-lived early deployment release	Migrate to 12.2(8)T or later Not Scheduled		
12.1YF	Short-lived early deployment release	Migrate to 12.1(5)YI or later Not Scheduled		
12.1YI	Short-lived early deployment release	Migrate to 12.2(2)XN or later Not Scheduled		
12.2-based Releases		Rebuild	Interim**	Maintenance
12.2	General deployment release for all platforms	12.2(6b)	12.2(7.4)	12.2(7)
12.2B	Early Deployment Broadband Release	12.2(4)B3	12.2(7.6)B	

12.2BC	Early Deployment Broadband Release uBR7000 and uBR10000	12.2(8)BC1		
12.2DA	Early Deployment Release: xDSL	12.2(6.8a)DA		12.2(7)DA
12.2DD	Specific Technology Early Deployment release for 7200 and 7400	Not Scheduled		
12.2S	S SLOB	Migrate to 12.2(4)BI or later	12.2(7.4)S	
12.2T	General deployment release for all platforms		12.2(7.4)T	12.2(8)T
12.2XA	Early Deployment Release	Not Scheduled		
		Migrate to 12.2(4)T or 12.2(2)XB		
12.2XB	Early Deployment Release	12.2(2)XB4 Available 2002–July		
12.2XD	ICS7750, 820, soho70	12.2(1)XD4		Not planned, migrate to 12.2(8)T or later
12.2XE	806, 820, soho78	12.2(1)XE3		Not planned, migrate to 12.2(8)T or later
12.2XF	DOCSYS support, uBR7100, uBR7200, uBR10000	Not Scheduled		
12.2XG	IAD2400/2600/3600	Migrate to 12.2(4)BC1		
		Not Scheduled		
		Migrate to 12.2(8)T		
12.2XH	1700, 800, 820, soho70	12.2(2)XH3		Not planned, migrate to 12.2(8)T
12.2XI	Early Deployment Release 820/SOHO	12.2(2)XI2		Not planned, migrate to 12.2(12)T
12.2XJ	1700	Not Scheduled		
		Migrate to 12.2(4)YB		

12.2XK	Early Deployment Release 820/SOHO	12.2(2)XK3		Not planned, migrate to 12.2(12)T
12.2XL	1700, 820, 800, SOHO70	12.2(4)XL5 Available 2002–June		Not planned, migrate to 12.2(12)T
12.2XM	Early Deployment Release	12.2(4)XM4		
12.2XN	Early Deployment Release for enhanced MGCP support, selected platforms	Not Scheduled		
		Upgrade recommended to a release yet to be determined		
12.2XQ	1720, 1750, 1752	Not Scheduled		
		Migrate to 12.2(4)YB or later		
12.2XR	Short-lived early deployment release	Not Scheduled		
		Migrate to 12.2(4)XR or later		
12.2XS	Short-lived early deployment release	Not Scheduled		
		Migrate to 12.2(6) or later		
12.2XT	Short-lived early deployment release	Not Scheduled		
		Migrate to 12.2(8)T or later		
12.2XW	Short-lived early deployment release	Not Scheduled		
		Migrate to 12.2(4)YB or later		
12.2YA	Early Deployment Release	12.2(4)YA2		
12.2YB	Short-lived early deployment release	Not Scheduled		
		Upgrade recommended to yet to be determined release		
12.2YC	Short-lived early deployment release	Not Scheduled		
		Migrate to 12.2(13)T or later		
12.2YD	Broadband suport for 7200	Not Scheduled		
		Migrate to 12.2(8)B or later		
12.2YF	Short-lived early deployment release	Not Scheduled		
		Upgrade recommended to yet to be determined release		
12.2YG	Early Deployment Release			12.2(4)YG
12.2YH	1700, 8xx, soho7x, ICS7700			12.2(4)YH

Notes

* All dates are estimates and subject to change.

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

Workarounds

It is possible to mitigate this vulnerability in two ways:

- Block all SSH connections on the border on your network, or
- On each individual device allow SSH connections only from the required IP addresses and block all others.

Blocking all SSH connections, and all other protocols that are not supposed to come from the outside, on the network edge should be an integral part of the network security best practice.

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

Publicly available malicious software is known to trigger this defect. Scanning for Unix hosts running vulnerable versions of SSH has been prevalent and such a scan may trigger this vulnerability.

Cisco PSIRT is aware of a few customers who experienced problems related to this vulnerability, however we do not have any evidence that these devices were targeted directly.

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-20020627-ssh-scan.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 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 1.0	2002-June-27	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: Jun 27, 2002

Document ID: 24862
