

Cisco Security Advisory: SSH Malformed Packet Vulnerabilities

Document ID: 29581

Advisory ID: cisco-sa-20021219-ssh-packet

<http://www.cisco.com/warp/public/707/cisco-sa-20021219-ssh-packet.shtml>

Revision 1.7

Last Updated 2005 October 19 2100 UTC (GMT)

For Public Release 2002 December 19 2300 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 Cisco products containing support for the Secure Shell (SSH) server are vulnerable to a Denial of Service (DoS) if the SSH server is enabled on the device. A malformed SSH packet directed at the affected device can cause a reload of the device. No authentication is necessary for the packet to be received by the affected device. The SSH server in Cisco IOS® is disabled by default.

Cisco will be making free software available to correct the problem as soon as possible.

The malformed packets can be generated using the SSHredder test suite from Rapid7, Inc. Workarounds are available. The Cisco PSIRT is not aware of any malicious exploitation of this vulnerability.

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20021219-ssh-packet.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

Multiple Cisco products which contain support for an SSH server are vulnerable if the SSH server is enabled.

Cisco products which are vulnerable include:

- Cisco Routers and Catalyst Switches running affected versions of Cisco IOS shown in the Software Version and Fixes section below
- Cisco Content Service Switch Models CSS11501, CSS11503, and CSS11506 running Cisco WebNS 5.10, 5.20, or 7.10
- Cisco Aironet 1200 Series Access Points running 12.00T or 12.01T
- Cisco Aironet 350 Series Access Points running 12.00T or 12.01T
- Cisco Aironet 340 Series Access Points running 12.00T or 12.01T
- Cisco Aironet 350 Series Wireless Bridges running 12.00T or 12.01T
- Cisco PIX Firewall
- Cisco ONS products: ONS15454, ONS15327 and ONS15600
- Firewall Services Module (FWSM) for Cisco Catalyst 6500 Switches and Cisco 7600 Series Routers

Products Confirmed Not Vulnerable

Cisco products which contain SSH server functionality that are **confirmed not to be vulnerable** include:

- Cisco Catalyst Switches running Cisco CatOS
- Cisco VPN3000 series concentrators
- Cisco Secure Intrusion Detection System (NetRanger) appliance
- Cisco Secure Intrusion Detection System Catalyst Module
- Cisco SN5400 Series Storage Routers
- CiscoWorks 1105 Wireless LAN Solution Engine (WLSE)
- CiscoWorks 1105 Hosting Solution Engine (HSE)
- Cisco ONS products: ONS15310
- Cisco ONS products: ONS15530, ONS15540

Details

A suite of crafted packets has been developed to test implementations of the Secure Shell (SSH) protocol. If the SSH server has been enabled, several of the test cases cause a forced reload of the device before the authentication process is called. Each time an SSH connection attempt is made to a affected Cisco device with one of the crafted packets, the device may hang or reboot.

Cisco IOS Software

The SSH server feature is available in the following Cisco IOS release trains: 12.0S, 12.0ST, 12.1T, 12.1E, 12.2, 12.2T, 12.2S. All releases which have the SSH server feature are vulnerable when the SSH server is enabled by issuing the command **crypto key generate rsa** in configuration mode.

All products running vulnerable versions of Cisco IOS except the Cisco 3550 will automatically reload and resume service following the crash. The Cisco 3550 will not reload, and will require manual intervention to resume normal processing.

Multiple Cisco IOS defects have been discovered. They are documented as CSCdz60229, CSCdy87221 and CSCdu75477.

Cisco Security Advisory: SSH Malformed Packet Vulnerabilities

Cisco Content Switching Software

Cisco Content Services Switches running vulnerable versions of Cisco WebNS software will reload and resume services.

This Cisco defect is documented in DDTS CSCdz62330.

Cisco Aironet Software

The SSH server feature was introduced as a feature in version 12.00T of the Aironet Software. Only versions 12.00T and 12.01T are vulnerable. Cisco Aironet Access Point devices running these vulnerable versions of Cisco Aironet software will reload and resume services.

This Cisco defect is documented in DDTS CSCdz66748.

Cisco PIX Firewall

A malformed SSH packet may cause the PIX to reload. In some circumstances, using CiscoWorks 2000 to monitor the PIX via SSH, can also cause the PIX to reload.

This Cisco defect is documented in DDTS CSCdz07673

Cisco ONS Products

A malformed SSH packet may cause the ONS product to reload. The SSH server feature was introduced as a feature in version 4.6.0 of the ONS System Software. Versions 4.6.0, 4.6.1 and 4.7.0 are vulnerable.

This Cisco defect is documented in DDTS CSCed38362.

Cisco Firewall Services Module (FWSM)

A malformed SSH packet may cause the FWSM to reload. In some circumstances, using CiscoWorks 2000 to monitor the FWSM via SSH, can also cause the FWSM to reload.

This Cisco defect is documented in DDTS CSCeb16775.

Impact

The vulnerability can be exploited to make an affected product unavailable for several minutes while the device reloads. Once it has resumed normal processing, the device is still vulnerable and can be forced to reload repeatedly.

Software Versions and Fixes

Cisco IOS Software

The SSH server feature is available beginning in the following Cisco IOS releases: 12.0(5)S, 12.0(16)ST, 12.1(1)T, 12.1(5a)E, 12.2(1), 12.2(1)T, 12.2(1)S. All of these versions are vulnerable if the SSH feature is enabled.

Each row of the Cisco IOS software table (below) 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 (the "First Fixed Release") and the anticipated date of availability for each are listed in the "Rebuild," "Interim," and "Maintenance" columns. A device running a release in the given train that is earlier than the release in a specific column (less than the First Fixed Release) is known to be vulnerable. The release should be upgraded at least to the indicated release or a later version (greater than or equal to the First Fixed Release label). When selecting a release, keep in mind the following definitions:

Maintenance

Most heavily tested, stable, and highly recommended release of a release train in any 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 repair the vulnerability.

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 TAC.

In all cases, customers should exercise caution to confirm that the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new software release. If the information is not clear, contact the Cisco TAC for assistance as shown in the Obtaining Fixed Software section below.

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

The fixes will be available at the Software Center located at <http://www.cisco.com/tacpage/sw-center/>.

For software installation and upgrade procedures, see http://www.cisco.com/warp/public/130/upgrade_index.shtml.

For a current view of all posted and repaired images for Cisco IOS, please check the listing available to registered CCO users at:

Train or Release	Description or Platform	Availability of First Fixed Releases*		
		Rebuild	Interim**	Maintenance
12.0S	Core/ISP support: GSR, RSP, c7200	12.0(21)S6		
		2003-Jan-27		
		12.0(22)S4		
		2003-Mar		

		12.0(23)S2		
		2003-Feb-17		
12.0ST	Early Deployment release	12.0(20)ST7		
		2003-Jan-27		
		12.0(21)ST6		
		2003-Feb-03		
12.1 Releases		Rebuild	Interim**	Maintenance
12.1E	Early Deployment release	12.1(13)E3		
		On CCO		
		12.1(14)E1		
		2003-Feb		
12.1EA	Early Deployment release	12.1(13) EA1		
12.1T	Early Deployment release all major platforms	2003-Mar Vulnerable		
12.2 Releases		Not Planned	Interim**	Maintenance
12.2	Major release for all platforms	Rebuild		
		12.2(12b)		
		On CCO		
		12.2(13a)		
		2003-Feb-07		
12.2S	Core ISP support			12.2(14)S
				2003-Jan-27
12.2T	Early deployment release all major platforms	12.2(11)T3		
		On CCO		
		12.2(13)T1		
NOTES:		2003-Feb-03		
* All dates are tentative and subject to change.				
** Interim releases receive less testing than Maintenance or Rebuild releases. Interim release labels are provided to identify vulnerable pre-existing Interim releases. A first fixed Interim release should be used only when no other suitable release is available.				

Cisco Content Switching Software

This vulnerability is fixed in the Cisco WebNS software which, according to its current schedule, will be available for download in January 2003. Interim Software releases of 5.20.0.06s and 7.10.0.06s are available now for download.

Cisco Aironet Software

This vulnerability is fixed in the Cisco Aironet software rebuild version 12.01T1. This software is expected to be available in late January 2003 and will be available for download from the Software Center.

Cisco PIX Firewall

This vulnerability is fixed in software versions 6.0(4.101), 6.1(5), 6.2(3) and 6.3(1).

Cisco ONS Products

This vulnerability is fixed in software versions 4.6.2, 5.0.0 and later releases.

Cisco Firewall Services Module (FWSM)

This vulnerability is first fixed in software version 2.2(1).

Workarounds

Cisco IOS Software

Workarounds consist of disabling the SSH server, removing SSH as a remote access method, permitting only trusted hosts to connect to the server, and blocking SSH traffic to the device completely via external mechanisms.



Caution: The following workaround will have undesirable side effects for IPSEC sessions that terminate on the device that use RSA key pairs for device authentication, or that use certificates based on those RSA key pairs. IPSEC sessions using other authentication methods will not be affected.

For Cisco IOS the SSH server can be disabled by applying the command **crypto key zeroize rsa** while in configuration mode. The SSH server is enabled automatically upon generating an RSA key pair. Zeroing the RSA keys is the only way to completely disable the SSH server.

Access to the SSH server on Cisco IOS may also be disabled via removing SSH as a valid transport protocol. This can be done by reapplying the **transport input** command with 'ssh' removed from the list of permitted transports on VTY lines while in configuration mode. For example:

```
line vty 0 4
  transport input telnet
end
```

If SSH server functionality is desired, access to the server can be restricted to specific source IP addresses or blocked entirely through the use of Access Control Lists (ACLs) on the VTY lines as shown in the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat2950/1219ea1/scg/swacl.htm#xtocid14>

More information on configuring ACLs can be found on Cisco's public website:

<http://www.cisco.com/warp/public/707/confaccesslists.html>

An example of a VTY access-list can be found here:

```
access-list 2 permit 10.1.1.0 0.0.0.255
access-list 2 deny any

line vty 0 4
access-class 2 in
end
```

Cisco Aironet Software

Cisco Aironet Access Points offer an IP Port Filter feature which may be used to mitigate an attack against an access point. Information on the configuration of IP Port filters can be found in the Access Point Configuration Guide:

http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo_350/accsspts/ap350scg/ap350ch5.htm

You may also block inbound SSH connections for your device with an external packet filtering device such as a firewall or a router that blocks traffic to TCP port 22.

Cisco PIX Firewall

Restrict access to the PIX SSH interface to allow connections only from trusted hosts and/or use HTTPS instead. Have CiscoWorks use Telnet to contact the PIX and restrict access to the PIX Telnet interface to allow connections only from the CiscoWorks workstation.

Cisco ONS Products

Block inbound SSH connections for the node with an external packet filtering device such as a firewall or a router that blocks traffic to TCP port 22.

Cisco Firewall Services Module (FWSM)

Restrict access to the FWSM SSH interface to allow connections only from trusted hosts and/or use HTTPS instead. Have CiscoWorks use Telnet to contact the PIX and restrict access to the PIX Telnet interface to allow connections only from the CiscoWorks workstation.

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

Cisco Security Advisory: SSH Malformed Packet Vulnerabilities

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 PSIRT is not aware of any malicious exploitation of this vulnerability. This suite of crafted packets from Rapid7, Inc. has been publicly announced via CERT/CC advisory CA-2002-36, and is available from the researcher's website. Cisco was initially listed in the CERT/CC advisory as not vulnerable based on initial testing of the suite, however upon continued internal testing it was determined that some products were vulnerable.

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 website at <http://www.cisco.com/warp/public/707/cisco-sa-20021219-ssh-packet.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
- full-disclosure@lists.netsys.com
- first-teams@first.org (includes CERT/CC)
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- comp.dcom.sys.cisco
- Various internal Cisco mailing lists

Future updates of this notice, if any, will be placed on Cisco's worldwide web. Users concerned about this problem are encouraged to check the URL given above for any updates.

Revision History

Revision Number 1.7	2005-October-19	Added Cisco Firewall Services Module (FWSM) to the Affected Products, Details, Software Versions and Fixes, and Workarounds sections.
Revision Number 1.6	2005-October-12	Added Cisco ONS product references to the Affected Products, Details, Software Versions and Fixes, and Workarounds sections.
Revision Number 1.5	2003-October-28	Updated entry for Software Release 12.1EA
Revision Number 1.4	2003-October-13	Corrected status for Cisco PIX Firewall - changed to affected.

Revision Number 1.3	2003–January–24	Updated fixed software for Aironet devices, status
Revision Number 1.2	2003–January–16	changed to Final. Updated list of affected products and fixed software to include Content Service Switches and Wireless Access Points
Revision Number 1.1	2002–December–20	Updated list of affected products to include HSE and
Revision Number 1.0	2002–December–19	WLSE 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: Oct 19, 2005

Document ID: 29581
