

# Cisco Security Advisory: Multiple SSH Vulnerabilities

Document ID: 8118

Advisory ID: cisco-sa-20010627-ssh

<http://www.cisco.com/warp/public/707/cisco-sa-20010627-ssh.shtml>

## Revision 1.6

Last Updated 2001 November 12 2030 UTC (GMT)

For Public Release 2001 June 27 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

Four different Cisco product lines are susceptible to multiple vulnerabilities discovered in the Secure Shell (SSH) protocol version 1.5. These issues have been addressed, and fixes have been integrated into the Cisco products that support this protocol.

By exploiting the weakness in the SSH protocol, it is possible to insert arbitrary commands into an established SSH session, collect information that may help in brute force key recovery, or brute force a session key.

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 products are vulnerable. It is possible to mitigate this vulnerability by preventing, or having control over, the interception of SSH traffic.

Cisco IOS is not vulnerable to any of known exploits that are currently used to compromise UNIX hosts. For the warning regarding increased scanning activity for hosts running SSH consult CERT/CC

This advisory will be posted at: <http://www.cisco.com/warp/public/707/cisco-sa-20010627-ssh.shtml>.

## Affected Products

### Vulnerable Products

The following table depicts the affected products categories.

Product Category	CRC-32	Traffic analysis	Key recovery
IOS	Vulnerable check <b>CSCdt96253</b>	Vulnerable <b>CSCdt57231</b>	Vulnerable <b>CSCdu37371</b>
PIX	Vulnerable <b>CSCdt73353</b>	Not vulnerable	Not vulnerable
VPN3000	Not vulnerable	Not vulnerable	Not vulnerable
Catalyst 6000	Vulnerable	Vulnerable	Not
CSS 11000	Vulnerable <b>CSCdt72996</b> <b>CSCdv34668</b>	Vulnerable <b>CSCdt55357</b> <b>CSCdv34676</b>	vulnerable <b>CSCdv34679</b>

Per product category, the following software releases are vulnerable:

IOS	All 12.0 and later releases that include support for SSH.
PIX	5.2(5) and 5.3.(1)
CatOS	6.2(0.110)
VPN3000	Not vulnerable
CSS 11000	All WebNS releases prior, but excluding, versions: R4.01 B42s, R4.10 B22s, R5.0 B11s, R5.01 B6s

### Products Confirmed Not Vulnerable

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

## Details

An implementation of SSH in multiple Cisco products are vulnerable to three different vulnerabilities. These vulnerabilities are:

- **CRC-32 integrity check vulnerability** — This vulnerability has been described in a CORE SDI S.A. paper entitled "An attack on CRC-32 integrity checks of encrypted channels using CBC and CFB modes", which can be found at <http://www.core-sdi.com/soft/ssh/ssh.pdf>. In order for this attack to succeed, an attacker must possess one or two known ciphertext/plaintext pairs. This should not be difficult since every session starts with a greeting screen which is fixed and which can be determined. This also implies that an attacker must be somewhere along the session path in order to be able to sniff the session and collect corresponding ciphertext. For further technical details, see <http://www.core-sdi.com/soft/ssh/ssh.pdf>. While fixing this vulnerability, we have not made the implementation mistake described by VU#945216 (see <http://www.kb.cert.org/vuls/id/945216>) which is being actively exploited.
- **Traffic analysis** — This issue has been described in an analysis jointly made by Dug Song and Solar Designer. It can be found at: <http://www.openwall.com/advisories/OW-003-ssh-traffic-analysis.txt>, and is entitled "Passive Analysis of SSH (Secure Shell) Traffic". To exploit this vulnerability, an attacker must be able to capture packets. When sending a packet using the SSH protocol, it is padded to the next 8-byte boundary, but the exact length of the data (without the padding) is sent unencrypted. The timing between packets may yield additional information, such as the relative position of a letter on the keyboard, but that depends on overall jitter in the network and the typing habits of the person. For additional information, please see <http://www.openwall.com/advisories/OW-003-ssh-traffic-analysis.txt>.
- **Key recovery in SSH protocol 1.5** — This has been discovered by CORE SDI S.A. and the paper describing it can be viewed at <http://www.securityfocus.com/archive/1/161150>. The subject line is "SSH protocol 1.5 session key recovery vulnerability". In order to exploit this vulnerability, an attacker must be able to sniff the SSH session and be able to establish a connection to the SSH server. In order to recover the server key, an attacker must perform an additional  $2^{20} + 2^{19} = 1572864$  connections. Since the key has a lifespan of about an hour, this means that an attacker must perform around 400 connections per second. For further details, please see <http://www.securityfocus.com/archive/1/161150>.

## Impact

This section describes the impact of these vulnerabilities.

- **CRC-32 integrity check vulnerability** — By exploiting this protocol weakness, the attacker can insert arbitrary commands in the session after the session has been established.
- **Traffic analysis** — This vulnerability exposes the exact lengths of the passwords used for login authentication. This is only applicable to an interactive session that is being established over the tunnel protected by SSH. This can significantly help an attacker in guessing the password using the brute force attack.
- **Key recovery in SSH protocol 1.5** — This vulnerability may lead to the compromise of the session key. Once the session key is determined, the attacker can proceed to decrypt the stored session using any implementation of the crypto algorithm used. This will reveal all information in an unencrypted form.

## Software Versions and Fixes

The following software releases contain fixes for all vulnerabilities.

For **CSS 11000** family, all vulnerabilities are fixed in the following software releases:

WebNS	R4.01 B42s, R4.10 B22s, R5.0 B11s, R5.01 B6s
-------	--

For **Catalyst 6000** switches, all vulnerabilities are fixed in the following CatOS releases.

CatOS	6.1(2.13), 6.2(0.111) and 6.3(0.7)PAN
-------	---------------------------------------

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 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 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	Early Deployment (ED) for all platforms		5.2(5)203 Available through TAC	5.2.(6) Available in August
5.3	Early Deployment (ED) for all platforms		5.3(1)202 Available through TAC	5.3.(2) Available in August
6.x-based Releases				
		Rebuild	Interim**	Maintenance

6.0	Early Deployment (ED) for all platforms			6.0(1) Available
-----	---	--	--	------------------

For **Cisco IOS 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
12.0-based Releases				
12.0S	Core/ISP support: GSR, RSP, c7200			12.0(20)S 2001–November
12.1-based Releases				
12.1	General deployment release for all platforms	SSH not supported		
12.1AA	Dial support	SSH not supported		
12.1CX	Core/ISP support: GSR, RSP, c7200	SSH not supported		
12.1DA	xDSL support: 6100, 6200	SSH not supported		
12.1DB	Cisco IOS Software Release 12.1(1)DB supports Cisco?s 6400 Universal Access Concentrator			
12.1DC	Cisco IOS Software Release 12.1(1)DC supports Cisco?s 6400 Universal Access Concentrator			
12.1E	Core/ISP support: GSR, RSP, c7200			12.1(8a)E 2001–Jul–09
12.1EC	12.1EC is being offered to allow early support of new features on the uBR7200 platform, as well as future support for new Universal		12.1(6.5)EC3	

	Broadband Router headend platforms.			
12.1EX	Catalyst 6000 support			12.1(8a)E 2001-Jul-09
12.1EY	Cat8510c, Cat8510m, Cat8540c, Cat8540m, LS1010			12.1(6)EY
12.1EZ	Early Deployment (ED): special image	12.1(6)EZ2		
12.1T	Early Deployment(ED): VPN, Distributed Director, various platforms	Not Scheduled		
12.1XA	Early Deployment (ED): limited platforms	Upgrade recommended to 12.2(1b) Not Scheduled		
12.1XB	Early Deployment (ED): limited platforms	Upgrade recommended to 12.2(1b)		
12.1XC	Early Deployment (ED): limited platforms	Not Scheduled		
12.1XD	Early Deployment (ED): limited platforms	Upgrade recommended to 12.2(1b) Not Scheduled		
12.1XE	Early Deployment (ED): limited platforms	Upgrade recommended to 12.2(1b)		
12.1XF	Early Deployment (ED): 811 and 813 (c800 images)	12.1(2)XF4 2001-July-09		
12.1XG	Early Deployment (ED): 800, 805, 820, and 1600	12.1(2)XF4 2001-July-09		
12.1XH	Early Deployment (ED): limited platforms	Not Scheduled		
12.1XI	Early Deployment (ED): limited platforms	Upgrade recommended to 12.2(1b) Not Scheduled		

Upgrade recommended to 12.2(1b)

12.1XJ	Early Deployment (ED): limited platforms	Not Scheduled		
12.1XK	Early Deployment (ED): limited platforms	Upgrade recommended to 12.1(5)YB4 SSH not supported		
12.1XL	Early Deployment (ED): limited platforms	Not Scheduled		
12.1XM	Short-lived early deployment release	Upgrade recommended to 12.2(1b) 12.1(4)XM4 2001-June-27		
12.1XP	Early Deployment (ED): 1700 and SOHO	12.1(3)XP4		
12.1XQ	Short-lived early deployment release	Not Scheduled		
12.1XR	Short-lived early deployment release	Upgrade recommended to 12.2(1b) 12.1(5)XR2		
12.1XS	Short-lived early deployment release	12.1(5)XS2 2001-July		
12.1XT	Early Deployment (ED): 1700 series	12.1(3)XT3		
12.1XU	Early Deployment (ED): limited platforms	12.1(5)XU1		
12.1XV	Short-lived early deployment release	12.1(5)XV3 2001-July		
12.1XW	Short-lived early deployment release	SSH not supported		
12.1XX	Short-lived early deployment release	SSH not supported		
12.1XY	Short-lived early deployment release	12.1(5)XY6 2001-July		
12.1XZ	Short-lived early deployment release	SSH not supported		
12.1YA		Not Scheduled		

	Short-lived early deployment release	Upgrade recommended to 12.2(2)XB 2001–August		
12.1YB	Short-lived early deployment release	12.1(5)YB4		
12.1YC	Short-lived early deployment release	12.1(5)YC1		
12.1YD	Short-lived early deployment release	12.1(5)YD2 2001–June–25		
12.1YF	Short-lived early deployment release	12.1(5)YF2		
12.2-based Releases		Rebuild	Interim*	Maintenance
12.2	General deployment release for all platforms	12.2(1b)	12.2(1.1)	12.2(3) 2001–August
12.2T	General deployment release for all platforms		12.2(2.2)T	
12.2XA	SPLOB			12.2(2)XA 2001–July–02
12.2XD	Short-lived early deployment release	12.2(1)XD1		
12.2XE	Short-lived early deployment release			12.2(1)XE
12.2XH	Short-lived early deployment release			12.2(1)XH 2001–June–25
12.2XQ	Short-lived early deployment release			12.2(1)XQ 2001–June–23
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

There are no workarounds for these vulnerabilities.

## 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

All three vulnerabilities are publicly known. Please see the Details section for the original announcements.

The Cisco PSIRT is not aware of malicious use of the vulnerabilities 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 Web site at <http://www.cisco.com/warp/public/707/cisco-sa-20010627-ssh.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](mailto:cust-security-announce@cisco.com)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [first-teams@first.org](mailto:first-teams@first.org) (includes CERT/CC)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [comp.dcom.sys.cisco](mailto:comp.dcom.sys.cisco)
- [firewalls@lists.gnac.com](mailto:firewalls@lists.gnac.com)
- Various internal Cisco mailing lists

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 1.6	2001-Nov-12	Updated information regarding vulnerability of UNIX hosts in Summary section and implementation mistake VU#945216 in Details section
Revision 1.5	2001-Oct-05	Updated SSH protocol version information in Summary section

Revision 1.4	2001–Oct–04	Updated maintenance release version and date for Cisco IOS software 12.0S train in Software Versions and Fixes section
Revision 1.3	2001–Sept–20	Updated information regarding CSS in Summary, Affected Products and <del>Software Versions and Fixes sections</del>
Revision 1.2	2001–Aug–08	Updated url in Details section
Revision 1.1	2001–June–28	Updated software availability date; added Traffic Analysis author
Revision 1.0	2001–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 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 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 14, 2007

Document ID: 8118

---