

Cisco Security Advisory: Cisco VPN 3000 Concentrator Vulnerabilities

Document ID: 42621

Advisory ID: cisco-sa-20030507-vpn3k

<http://www.cisco.com/warp/public/707/cisco-sa-20030507-vpn3k.shtml>

Revision 1.2

Last Updated 2003 May 08 0519 UTC (GMT)

For Public Release 2003 May 07 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

This advisory documents vulnerabilities for the Cisco VPN 3000 series concentrators and Cisco VPN 3002 Hardware Client. These vulnerabilities are documented as Cisco bug ID CSCea77143 (IPSec over TCP), CSCdz15393 (SSH), and CSCdt84906 (ICMP). There are workarounds available to mitigate the effects of these vulnerabilities. Upgrading to the latest version of code for the Cisco VPN 3000 series concentrators and Cisco VPN 3002 Hardware Client, version 4.0.1 and 3.6.7F, would protect against all of these documented vulnerabilities.

This advisory will be posted at <http://www.cisco.com/warp/public/707/cisco-sa-20030507-vpn3k.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

The Cisco VPN 3000 series concentrators are affected by these vulnerabilities. This series includes models 3005, 3015, 3030, 3060, 3080 and the Cisco VPN 3002 Hardware Client.

DDTS – Description	Affected Releases
CSCea77143 – enabling IPsec over TCP vulnerability	<ul style="list-style-type: none"> • 4.0.REL • 3.6.REL through 3.6.7E • 3.5.x • 3.1.x, 3.0.x and 2.x.x are NOT affected.
CSCdz15393 – malformed SSH initialization packet vulnerability	<ul style="list-style-type: none"> • 3.6.REL through 3.6.6 • 3.5.x • 3.1.x • 3.0.x • 2.x.x
CSCdt84906 – malformed ICMP traffic vulnerability	<ul style="list-style-type: none"> • 3.6.REL through 3.6.7 • 3.5.x • 3.1.x • 3.0.x • 2.x.x

To determine if a Cisco VPN 3000 series concentrator is running affected software, check the software revision via the web interface or the console menu.

Products Confirmed Not Vulnerable

These vulnerabilities do not affect the VPN Client software nor the Cisco VPN 5000 series concentrators. No other Cisco products are currently known to be affected by these vulnerabilities.

Details

This table provides details about these vulnerability.

DDTS – Description	Details
CSCea77143 – enabling IPsec over TCP vulnerability	<p>Enabling IPsec over TCP for a port on the VPN 3000 series concentrator allows TCP traffic on that port to traverse through the concentrator and reach the private network.</p> <p>For example, if one configures IPsec over TCP to use port 80 and the private network is routable to from the public network i.e. a workstation on the public network has the VPN 3000 series concentrator configured as the gateway for the private network IP address space, one can browse the web servers on the private network configured to serve port 80 from the workstation on the public network without any form of authentication. Another example, if IPsec over TCP was not configured for port 80 but was configured for its default port of 10000 and if there was a server listening for telnet connections on port 10000 on the private network, then one could telnet to that server from the workstation on the public network.</p>

	For more information on IPSec over TCP please refer to the documentation available at http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3000/4_0/config/tunnel.htm#1279809
CSCdz15393 – malformed SSH initialization packet vulnerability	A malformed SSH initialization packet sent during the initial SSH session setup may reload the VPN 3000 series concentrator.
CSCdt84906 – malformed ICMP traffic vulnerability	A flood of malformed ICMP packets could result in performance degradation on the VPN 3000 series concentrator and may even cause the concentrator to reload.

These vulnerabilities are documented in the Cisco [Bug Toolkit](#) ([registered](#) customers only) as Bug IDs CSCea77143, CSCdz15393, and CSCdt84906, and can be viewed after 2003 May 8 at 1600 UTC. To access this tool, you must be a registered user and you must be logged in.

The Inter networking Terms and Cisco Systems Acronyms online guides can be found at <http://www.cisco.com/univercd/cc/td/doc/cisintwk/>.

Impact

Successful exploitation of the vulnerability may result in the issues described in this table.

DDTS – Description	Impact
CSCea77143 – enabling IPSec over TCP vulnerability	Unintended access to the private network on the VPN 3000 series concentrator. This vulnerability enables one to access internal hosts on the IPSec over TCP configured ports.
CSCdz15393 – malformed SSH initialization packet vulnerability	This vulnerability can be exploited to initiate a Denial of Service on the VPN 3000 series concentrator.
CSCdt84906 – malformed ICMP traffic vulnerability	This vulnerability may cause a performance degradation on the VPN 3000 series concentrator and may even result in a Denial of Service.

Software Versions and Fixes

When considering software upgrades, also consult <http://www.cisco.com/go/psirt> and any subsequent advisories to determine exposure and a complete upgrade solution.

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 Technical Assistance Center ("TAC") or your contracted maintenance provider for assistance.

DDTS – Description	Fixed Releases
CSCea77143 – enabling IPsec over TCP vulnerability	<ul style="list-style-type: none"> • 4.0.1 and later • 3.6.7F and later • 3.1.x, 3.0.x and 2.x.x are NOT affected
CSCdz15393 – malformed SSH initialization packet vulnerability	<ul style="list-style-type: none"> • 4.0.REL and later • 3.6.7 and later
CSCdt84906 – malformed ICMP traffic vulnerability	<ul style="list-style-type: none"> • 4.0.REL and later • 3.6.7A and later

The procedure to upgrade to the fixed software version is detailed at <http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3000/>.

Workarounds

The Cisco PSIRT recommends that affected users upgrade to a fixed software version of code.

DDTS – Description	Workaround
CSCea77143 – enabling IPsec over TCP vulnerability	Add rules, to the filter for the private interface, that restrict outgoing traffic on ports configured for use by IPsec over TCP on the VPN concentrator. This would not stop the traffic from the public network reaching the VPN 3000 concentrator itself but would prevent the traffic from reaching the servers on the private network.
CSCdz15393 – malformed SSH initialization packet vulnerability	Restrict access to the SSH server on the VPN 3000 series concentrator by applying appropriate rules to the filters for the
CSCdt84906 – malformed ICMP traffic vulnerability	interfaces such that connections are permitted only from trusted client hosts. Only allow legitimate ICMP traffic to reach the VPN 3000 series concentrator's interface.

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 vulnerabilities described in this advisory.

These vulnerabilities were reported to PSIRT by internal development testing.

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-20030507-vpn3k.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 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 1.0	2003 May 7	Initial public release.
Revision 1.1	2003 May 7	Corrected the Affected Products table.
Revision 1.2	2003 May 8	Corrected the link in the Obtaining Fixed Software section.

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>.

