

# Cisco Security Advisory: Cisco VPN Client Multiple Vulnerabilities – Second Set

Document ID: 26833

Advisory ID: cisco-sa-20020905-vpnclient-vulnerability

<http://www.cisco.com/warp/public/707/cisco-sa-20020905-vpnclient-vulnerab>

## Revision 1.0

For Public Release 2002 September 05 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

Multiple vulnerabilities exist in the Cisco Virtual Private Network (VPN) Client software. These vulnerabilities are documented as Cisco Bug IDs CSCdt35749, CSCdt60391, CSCdw87717, CSCdx89416 and CSCdy37058. There are no workarounds available to mitigate the effects of these vulnerabilities.

This advisory will be posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20020905-vpnclient-vulnerability.shtml>.

## Affected Products

This section provides details on affected products.

## Vulnerable Products

The VPN Client software program runs on the following platforms.

- Microsoft Windows based PC.

- Red Hat Version 6.2 Linux (Intel), or compatible distribution, using kernel Version 2.2.12 or later. It does not support kernel Version 2.5.
- Solaris UltraSPARC running a 32-bit or a 64-bit kernel OS Version 2.6 or later.
- Mac OS X Version 10.1.0 or later.

DDTS Description	Affected Releases
CSCdt35749 – NETBIOS TCP packet vulnerability	<ul style="list-style-type: none"> <li>• earlier than 3.0.5</li> <li>• 2.x.x</li> </ul>
CSCdt60391 – Group passwords visible using utility program	<ul style="list-style-type: none"> <li>• earlier than 3.5.1C</li> <li>• 3.1.x</li> <li>• 3.0.x</li> <li>• 2.x.x</li> </ul>
CSCdw87717 – Concentrator certificate identity vulnerability	<ul style="list-style-type: none"> <li>• earlier than 3.5.1C</li> <li>• 3.1.x</li> <li>• 3.0.x</li> <li>• 2.x.x</li> </ul>
CSCdx89416 – Random number generation improvement	<ul style="list-style-type: none"> <li>• earlier than 3.5.2B</li> <li>• 3.1.x</li> <li>• 3.0.x</li> <li>• 2.x.x</li> </ul>
CSCdy37058 – TCP filter vulnerability	<ul style="list-style-type: none"> <li>• 3.6(Rel)</li> <li>• earlier than 3.5.4</li> <li>• 3.1.x</li> <li>• 3.0.x</li> <li>• 2.x.x</li> </ul>

## Products Confirmed Not Vulnerable

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

## Details

The VPN Client software program on a remote workstation, communicating with a Cisco VPN device on an enterprise network or with a service provider, creates a secure connection over the Internet. Through this connection you can access a private network as if you were an onsite user.

DDTS Description	Details
CSCdt35749 – NETBIOS TCP packet vulnerability	The VPN Client is vulnerable to NETBIOS TCP packets that have their source and destination ports set to 137 (NETBIOS Name Service). Upon receiving such a packet, the
CSCdt60391 – Group passwords visible using utility program	VPN Client crashes. There is a utility program under Windows that can decipher the group password field, which is shown as a series of asterisks (***) on the authentication property page
CSCdw87717 – Concentrator certificate identity vulnerability	of the VPN Client. When a VPN Client connects to a VPN Concentrator using certificates, the VPN Client does not have the ability to verify that specific certificate DN fields match in the
CSCdx89416 – Random number generation improvement	certificate received from the VPN Concentrator. The random number generation process in the VPN Client software has been significantly
CSCdy37058 – TCP filter vulnerability	improved to increase the randomness of the generated numbers. It is possible to get the VPN Client, which is configured for all tunnel mode (split tunneling disabled mode), to acknowledge a TCP packet via the tunnel–assigned IP, when the packet is sent to it from outside the tunnel. The 3.5.x releases are protected against this vulnerability if the firewall is configured to be in "always on" mode. The 3.6(Rel) release is vulnerable even when the firewall is in "always on" mode.

These vulnerabilities are documented in the Cisco Bug Toolkit as Bug IDs CSCdt35749, CSCdt60391, CSCdw87717, CSCdx89416 and CSCdy37058, and can be viewed after 2002 September 6 at 1500 UTC. To access this tool, you must be a registered user and you must be logged in.

## Impact

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

DDTS Description	Impact
------------------	--------

CSCdt35749 – NETBIOS TCP packet vulnerability	This vulnerability can be exploited to initiate a denial-of-service attack.
CSCdt60391 – Group passwords visible using utility program	Unintended disclosure of the group password.
CSCdw87717 – Concentrator certificate identity vulnerability	This vulnerability could be exploited to initiate a man-in-the-middle attack.
CSCdx89416 – Random number generation improvement	Improvement in the randomness of random numbers generated for use by the VPN Client.
CSCdy37058 – TCP filter vulnerability	This vulnerability could be exploited to leak information about the VPN Client workstation.

## 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
CSCdt35749 – NETBIOS TCP packet vulnerability	<ul style="list-style-type: none"> <li>• 3.6(Rel) or later</li> <li>• 3.5(Rel) or later</li> <li>• 3.1(Rel) or later</li> <li>• 3.0.5 or later</li> </ul>
CSCdt60391 – Group passwords visible using utility program	<ul style="list-style-type: none"> <li>• 3.6(Rel) or later</li> <li>• 3.5.1C or later</li> </ul>

CSCdw87717 – Concentrator certificate identity vulnerability	<ul style="list-style-type: none"> <li>• 3.6(Rel) or later</li> <li>• 3.5.1C or later</li> </ul>
CSCdx89416 – Random number generation improvement	<ul style="list-style-type: none"> <li>• 3.6(Rel) or later</li> <li>• 3.5.2B or later</li> </ul>
CSCdy37058 – TCP filter vulnerability	<ul style="list-style-type: none"> <li>• 3.6.1 or later</li> <li>• 3.5.4 or later</li> </ul>

The procedure to upgrade on the various platforms to the fixed software version is detailed in the documentation available at <http://www.cisco.com/univercd/cc/td/doc/product/vpn/client/>.

## Workarounds

Workarounds are described in this table.

DDTS Description	Workaround
CSCdt35749 – NETBIOS TCP packet vulnerability	There is no workaround.
CSCdt60391 – Group passwords visible using utility program	There is no workaround.
CSCdw87717 – Concentrator certificate identity vulnerability	There is no workaround.
CSCdx89416 – Random number generation improvement	Not applicable.
CSCdy37058 – TCP filter vulnerability	There is no workaround.

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

## 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

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 and customers.

## 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-20020905-vpnclient-vulnerability.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 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 1.0	<del>2002-September-05</del>	<del>Initial public release.</del>
--------------	------------------------------	------------------------------------

## 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/go/psirt>. This includes instructions for press inquiries regarding Cisco security advisories.

---

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

---

Updated: Sep 05, 2002

Document ID: 26833

---