

# [NEWS] Cisco VPN Client Multiple Vulnerabilities

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-08/0044.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 08/13/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: Tue, 13 Aug 2002 15:54:48 +0200 (CEST)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

-----

Cisco VPN Client Multiple Vulnerabilities

---

## SUMMARY

Multiple vulnerabilities exist in the Cisco Virtual Private Network (VPN) Client software. Exploitation of these vulnerabilities prevents the Cisco VPN Client software program from functioning correctly.

These vulnerabilities are documented as Cisco bug ID CSCdy26045. There are no workarounds available to mitigate the effects of these vulnerabilities.

## DETAILS

Affected 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 kernel OS Version 2.6 or later.
- \* Mac OS X Version 10.1.0 or later.

All VPN Client software programs, earlier than version 3.6 and earlier than version 3.5.4, on all platforms are affected by this vulnerability.

This includes the previous Cisco Secure VPN Client and the Cisco VPN 3000 Client software programs.

## Securiteam: [NEWS] Cisco VPN Client Multiple Vulnerabilities

Cisco VPN 5000 Client software programs are not affected by this vulnerability.

No other Cisco product is currently known to be affected by this vulnerability.

### 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 on-site user.

The VPN Client software program has been found to have the following vulnerabilities:

- \* An Internet Key Exchange (IKE) packet with a Security Parameter Index (SPI) payload containing more than 16 bytes causes a buffer overflow in the VPN client software.

- \* An IKE packet with more than 57 valid payloads causes a buffer overflow in the VPN Client software.

- \* When the VPN Client software receives a specially crafted packet with a zero length payload it causes the VPN Client software to use 100% of CPU resources on the workstation.

These vulnerabilities are documented as Cisco bug ID CSCdy26045, which requires a CCO account to view. CSCdy26045 can be viewed after 2002 August 13 at 1500 UTC.

### Impact:

When the vulnerabilities are exploited, they prevent the Cisco VPN Client software program from functioning correctly. The Cisco VPN Client software program's availability may be impacted. There is no impact to the confidentiality and integrity of the data.

### Software Versions and Fixes:

This vulnerability has been fixed in Cisco VPN Client version 3.6 or later, which is now available for download. The fix for this vulnerability will also be integrated in VPN Client version 3.5.4 or later, and will be available for download by September 30, 2002.

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

### Obtaining Fixed Software:

Cisco is offering free software upgrades to address this vulnerability for all affected customers. Customers may only install and expect support for the feature sets they have purchased.

## Securiteam: [NEWS] Cisco VPN Client Multiple Vulnerabilities

Customers with service contracts should contact their regular update channels to obtain the free software upgrade identified via this advisory. For most customers with service contracts, this means that upgrades should be obtained through the Software Center on Cisco's worldwide website at <http://www.cisco.com/kobayashi/sw-center/>

Customers whose Cisco products are provided or maintained through a prior or existing agreement with third-party support organizations such as Cisco Partners, authorized resellers, or service providers should contact that support organization for assistance with obtaining the free software upgrade(s).

Customers who purchased directly 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 obtain fixed software by contacting the Cisco Technical Assistance Center (TAC) using the contact information listed below. In these cases, customers are entitled to obtain an upgrade to a later version of the same release or as indicated by the applicable corrected software version in the Software Versions and Fixes section (noted above).

Cisco 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)

See <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.

Please have your product serial number available and give the URL of this advisory as evidence of your entitlement to a free upgrade.

Please do not contact either "[psirt@cisco.com](mailto:psirt@cisco.com)" or "[security-alert@cisco.com](mailto:security-alert@cisco.com)" for software upgrades.

Workarounds:

There are no workarounds for these vulnerabilities. The Cisco PSIRT recommends that affected users upgrade to a fixed software version of code.

### ADDITIONAL INFORMATION

The information has been provided by <mailto:psirt@cisco.com> Cisco PSIRT.

=====

Securiteam: [NEWS] Cisco VPN Client Multiple Vulnerabilities

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

[list-unsubscribe@securiteam.com](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====  
=====

**DISCLAIMER:**

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

- 
- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[NT] Unchecked Buffer in Jana Web Server (Method)"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)