

[NEWS] Buffer Overflow in UNIX VPN Client

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-06/0101.html>

From: support@securiteam.com

Date: 06/21/02

From: support@securiteam.com

To: list@securiteam.com

Date: Fri, 21 Jun 2002 21:41:47 +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.

Buffer Overflow in UNIX VPN Client

SUMMARY

A buffer overflow in the Cisco VPN Clients for Linux, Solaris, and Mac OS X platforms can be exploited locally to gain administrative privileges on the client system. The vulnerability can be mitigated by removing the "setuid" permissions on the vpnclient binary executable file. The Cisco VPN Clients for Windows platforms are not affected.

The vulnerability has been repaired in version 3.5.2. Cisco is making fixed software available free to affected customers. This issue is documented as CSCdx39290. Cisco is not aware of any public discussion or active exploitation of this vulnerability.

DETAILS

Affected Products:

This vulnerability affects versions 3.5.1 and earlier of the Cisco VPN Clients for Linux, Solaris, and Mac OS X platforms.

It does not affect the Cisco VPN Clients for any Windows platform. No other Cisco product is affected.

Details:

The Cisco VPN (Virtual Private Network) Client establishes an encrypted

Securiteam: [NEWS] Buffer Overflow in UNIX VPN Client

tunnel between a local system and a Cisco VPN Concentrator. The tunnel provides confidentiality and integrity for the data in transit, allowing a user on the local system to securely connect to a corporate network via a public, possibly untrusted network.

If an overly-long profile name is given as an argument to the `vpnclient` command, a buffer overflow occurs that overwrites return values on the system's stack. The contents of the overly-long profile name could be crafted to execute arbitrary instructions. The buffer overflow can only be exercised by executing the `vpnclient` command directly on the local system.

By default, the `vpnclient` command is installed on a UNIX-based system as a binary executable file with `setuid` permissions. Since `setuid` files execute with the effective permissions of "root", the administrative user of a UNIX-based system, the arbitrary instructions will execute with administrative permissions.

In lieu of installing fixed software, the vulnerability can be mitigated by removing the `setuid` permissions on the `vpnclient` binary executable file as shown below. This cannot prevent the buffer overflow from occurring, but limits the simple range of damage that could occur.

The problem has been resolved by adding better tests for buffer overflows and by removing unnecessary `setuid` permissions on executable files in the software package as provided. Note that the `cvpnd` daemon, another one of the binary executable files in the software package, retains `setuid` permissions to preserve its ability to change the configuration of the network interface. This capability is essential for establishing, managing, and removing a VPN connection.

This vulnerability is documented as CSCdx39290. Details can be viewed on-line by registered users of Cisco's website.

Impact:

The vulnerability could be exploited by a local user to execute arbitrary instructions. If the affected binary executable file is installed with `setuid` permissions, the instructions will execute with administrative permissions and could be used to modify any part of the system without authorization. The `setuid` permissions are set by default in the software package as supplied by Cisco.

Software Versions and Fixes:

This vulnerability was found and reported in the Cisco VPN Client version 3.5.1 for Linux, and has been confirmed internally in the Cisco VPN Client for Solaris and Mac OS X. It has been repaired in version 3.5.2 for those affected platforms and is available immediately. All previous versions on the affected platforms are considered vulnerable. The fixes will be carried forward into all future versions.

Obtaining Fixed Software:

Cisco is making fixed software available free of charge to all affected

Securiteam: [NEWS] Buffer Overflow in UNIX VPN Client

customers.

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 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 assistance with the upgrade, which should be free of charge.

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):

- * +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

See <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> for additional TAC contact information, including special localized telephone numbers, instructions, and e-mail addresses for use in various languages.

Please 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.

Please do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software upgrades.

Workarounds:

The vulnerability can be mitigated by removing setuid permissions on the vpnclient executable binary file using the chmod command on the affected file as follows:

```
/bin/chmod 755 /usr/local/bin/vpnclient
```

If unfixed versions of the software are re-installed at a later date or restored from backups, the workaround shown above must be executed again.

Note: The workaround shown above does not prevent the buffer overflow from occurring. It merely limits the range of the simple damage that can occur if the overflow is exploited. Customers are urged to upgrade to fixed versions of the software as soon as possible.

Securiteam: [NEWS] Buffer Overflow in UNIX VPN Client

Also note that the cvpnd binary executable file must retain setuid permissions in order to operate correctly. Customers are cautioned not to use wildcards to remove setuid permissions on files in the VPN Client software package.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:psirt@cisco.com>> Cisco Systems Product Security Incident Response Team.

=====

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

In order to subscribe to the mailing list, simply forward this email to: 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: "[TOOL] SHOUTcast Admin Password Bruteforce Tool"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)