

[NEWS] Cisco VPN3000 Gateway MTU Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-07/0040.html>

From: support@securiteam.com

Date: 07/11/02

From: support@securiteam.com

To: list@securiteam.com

Date: Thu, 11 Jul 2002 12:07:21 +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 VPN3000 Gateway MTU Overflow

SUMMARY

The Cisco <<http://www.cisco.com/univercd/cc/td/doc/pcat/3000.htm>> VPN3000 gateway lets remote client dictate which maximum MTU to use when sending back ESP frames, regardless of the transmitting capabilities of the physical medium (thus going over the frame buffer's size).

DETAILS

Vulnerable systems:

- * Cisco/VPN 3000 Concentrator with software vpn3000-3.5.Rel-k9.bin

Impact:

- * Oversized frames get silently discarded by equipments linked to the gateway's public interface and retransmissions occur.

- * Other disturbances or DoS against neighboring equipments may occur, especially as many IP stacks on routers, sniffers, etc are poorly implemented.

Technical details:

When a target sends back Ethernet frames with size close to the max Ethernet MTU (1500), the gateway encrypts the frames adding ESP headers and then tries to send a 1580-bytes (which is well over the 1500+- frame

Securiteam: [NEWS] Cisco VPN3000 Gateway MTU Overflow

size limit) frame back to the client.

Workaround:

For Windows-based OS (likely UNIX and Linux-based OS too), Cisco released a tool called

<http://www.cisco.com/univercd/cc/td/doc/product/vpn/client/3_1/admin/vcach5.htm> setMTU.exe that can prevent ill MTU negotiation from happening.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:porte10@free.fr>> porte10.

=====

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: "[NT] Cumulative Patch for SQL Server"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)