

[NEWS] Cisco VPN 3000 Concentrator DoS (Technical Details)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-02/msg00006.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 2 Feb 2006 10:39:56 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the S
- - promotion

The SecuriTeam alerts list - Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

- - - - -

Cisco VPN 3000 Concentrator DoS (Technical Details)

SUMMARY

"The Cisco VPN 3000 series concentrators are a family of purpose-built, remote access Virtual Private Network (VPN) platforms for data encryption and authentication." A malicious user may be able to send a crafted HTTP (Hypertext Transfer Protocol) packet to the concentrators which may cause the device to reload and drop user connections using the Cisco VPN 3000 Concentrator.

DETAILS

Vulnerable Systems:

- * Cisco VPN 3000 series concentrators version 4.7.0 and above
- * Cisco VPN 3000 series concentrators version 4.7.2 and prior
- * Cisco VPN 3000 series concentrators version 4.7REL.
- * Cisco VPN 3000 series concentrators version 4.7.2.B

Immune Systems:

- * Cisco VPN 3002 Hardware Client
- * Cisco IPsec VPN Services Module (VPNSM)
- * Cisco VPN 5000 Concentrators
- * Cisco PIX Firewalls
- * Cisco Adaptive Security Appliance (ASA)
- * Any Cisco device that runs Cisco's Internetwork Operating System (IOS)
- * Any Cisco device that runs Cisco's Catalyst Operating System (CatOS)
- * Cisco VPN 3000 series concentrators version 4.6.x and prior

The exploit involves sending a single small stream (less than 50 packets) of TCP/80 traffic to a Cisco VPN 3000 Concentrator appliance running the WebVPN service. After this occurs, all sessions currently accessing the

[NEWS] Cisco VPN 3000 Concentrator DoS (Technical Details)

appliance are dropped, and no further communication is possible until the system is powered down and restarted. No authentication or credentials are required to exercise this vulnerability.

By default, the WebVPN Service permits both tcp/80 (HTTP) and TCP/443 (HTTPS) inbound; the appliance performs a redirect from the HTTP query to the HTTPS. The vulnerability exists within the code base responsible for the redirect.

There are a few inaccuracies in the original Cisco advisory:

1 It states that this exploit may reload the affected device. In fact, the exploit never reloads the device. The exploit completely freezes the device, requiring that the power cord be pulled out and reinserted to restart.

2 It states that repeated exploitation of the vulnerability could result in a sustained Denial of Service. In fact, it is possible by performing the exploit once to be kept offline until the power can be manually recycled. The appliance is completely hung.

3. The advisory states that upgrading to firmware version 4.7.2B is sufficient to defend against this exploit. This is not the case. The original tests WERE performed against VPN 3000 appliances running 4.7.1 but subsequent tests show that 4.7.2B is also susceptible to this exploit. The only way to resolve this issue is to block tcp/80 via ACL or by disabling it on the WebVPN.

ADDITIONAL INFORMATION

The information has been provided by <mailto:eldons@xxxxxxxxxxxxx> Eldon Sprickerhoff.

The vendor advisory can be found at:

<http://www.cisco.com/warp/public/707/cisco-sa-20060126-vpn.shtml>

<http://www.cisco.com/warp/public/707/cisco-sa-20060126-vpn.shtml>

=====

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@xxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxx

=====

=====

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,