

Re: [VulnWatch] Cisco Security Advisory: Cisco VPN 3000 Concentrator Vulnerable to Crafted HTTP Attack

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2006-01/msg00039.html>

- *From:* Eldon Sprickerhoff <eldons@xxxxxxxxxxxxx>
 - *Date:* Tue, 31 Jan 2006 15:18:28 -0500 (EST)
-

With respect to:

<http://archives.neohapsis.com/archives/vulnwatch/2006-q1/0036.html>

I'm the person who discovered this particular Cisco VPN vulnerability (and divulged some details at the end of my talk at Shmoocon – not "Schmoocon" as the original advisory spells it).

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 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.

First, 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.

Second, 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.

Finally, 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

Re: [VulnWatch] Cisco Security Advisory: Cisco VPN 3000 Concentrator Vulnerable to Crafted HTTP Attack

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.

Further details (including some background) are available at:

<http://www.esentire.com/news/vuln-cisco-vpn.html>

EWS

- Prev by Date: [*\[VulnWatch\] Digital Armaments: Apache auth ldap module Multiple Format Strings Vulnerability*](#)
- Previous by thread: [*\[VulnWatch\] Cisco Security Advisory: Cisco VPN 3000 Concentrator Vulnerable to Crafted HTTP Attack*](#)
- Next by thread: [*\[VulnWatch\] \[Argeniss\] Oracle Database Buffer overflows vulnerabilities in public procedures of XDB.DBMS XMLSCHEMA{ INT}*](#)
- Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)

Re: [VulnWatch] Cisco Security Advisory: Cisco VPN 3000 Concentrator Vulnerable to Crafted HTTP Attack