

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

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2006-02/msg00000.html>

---

- *From:* Mike Iglesias <[iglesias@xxxxxxxxxxxxxxxxxxxxx](mailto:iglesias@xxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Tue, 31 Jan 2006 23:15:35 -0800
- 

> 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  
> 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.

FYI: I asked Cisco which version this bug was fixed in, and they said that 4.7.2(C) has the fix.

Mike Iglesias	Email:	iglesias@xxxxxxx
University of California, Irvine	phone:	949-824-6926
Network & Academic Computing Services	FAX:	949-824-2069