

US-CERT Technical Cyber Security Alert TA08-087B -- Cisco Updates for Multiple Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Cert/2008-03/msg00003.html>

- *From:* CERT Advisory <cert-advisory@xxxxxxxx>
 - *Date:* Thu, 27 Mar 2008 16:05:52 -0400
-

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

National Cyber Alert System

Technical Cyber Security Alert TA08-087B

Cisco Updates for Multiple Vulnerabilities

Original release date: March 27, 2007

Last revised: --

Source: US-CERT

Systems Affected

* Cisco IOS

Overview

Cisco has released Cisco Security Advisory [cisco-sa-20080326-bundle](#) to correct multiple vulnerabilities affecting Cisco IOS. Attackers could exploit these vulnerabilities to access sensitive information or cause a denial of service.

I. Description

Cisco Security Advisory [cisco-sa-20080326-bundle](#) addresses a number of vulnerabilities affecting Cisco IOS 12.0, 12.1, 12.2, 12.3, and 12.4. Further details are available in the US-CERT Vulnerability Notes Database.

II. Impact

The impacts of these vulnerabilities vary. Potential consequences include disclosure of sensitive information and denial of service.

III. Solution

Upgrade

These vulnerabilities are addressed in Cisco Security Advisory [cisco-sa-20080326-bundle](#).

IV. References

- * US-CERT Vulnerability Notes –
<<http://www.kb.cert.org/vuls/byid?searchview&query=cisco-sa-20080326-bundle>>
- * Cisco Security Advisory [cisco-sa-20080326-bundle](#) –
<<http://www.cisco.com/warp/public/707/cisco-sa-20080326-bundle.shtml>>
- * Cisco Security Advisory: Cisco IOS Virtual Private Dial-up Network Denial of Service Vulnerability –
<<http://www.cisco.com/warp/public/707/cisco-sa-20080326-pptp.shtml>>
- * Cisco Security Advisory: Multiple DLSw Denial of Service Vulnerabilities in Cisco IOS –
<<http://www.cisco.com/warp/public/707/cisco-sa-20080326-dlsw.shtml>>
- * Cisco Security Advisory: Cisco IOS User Datagram Protocol Delivery Issue For IPv4/IPv6 Dual-stack Routers –
<<http://www.cisco.com/warp/public/707/cisco-sa-20080326-IPv4IPv6.shtml>>
- * Cisco Security Advisory: Vulnerability in Cisco IOS with OSPF, MPLS VPN, and Supervisor 32, Supervisor 720, or Route Switch Processor 720 –
<<http://www.cisco.com/warp/public/707/cisco-sa-20080326-queue.shtml>>
- * Cisco Security Advisory: Cisco IOS Multicast Virtual Private Network (MVPN) Data Leak –
<<http://www.cisco.com/warp/public/707/cisco-sa-20080326-mvpn.shtml>>

The most recent version of this document can be found at:

<<http://www.us-cert.gov/cas/techalerts/TA08-087B.html>>

US-CERT Technical Cyber Security Alert TA08-087B -- Cisco Updates for Multiple Vulnerabilities

Feedback can be directed to US-CERT Technical Staff. Please send email to <cert@xxxxxxxx> with "TA08-087B Feedback VU#936177" in the subject.

For instructions on subscribing to or unsubscribing from this mailing list, visit <<http://www.us-cert.gov/cas/signup.html>>.

Produced 2008 by US-CERT, a government organization.

Terms of use:

<<http://www.us-cert.gov/legal.html>>

Revision History

March 27, 2008: Initial release

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.2.1 (GNU/Linux)

```
iQEVAwUBR+vjW/RFkHkM87XOAQLjnQf+PgUTq9wrF8th28Ur2qUgViOGFbNOzwbp
1Awpl1yGpNgsT2BVbdwo7ugfuQXMHiz8rnG/7Ovf5pr3FjI6l/3XRMFTpS/ZmF1W
m0e6H+vhJSmvJp02a4X9Rzm8Rq9jYda7SJHAFiiblxMSKOuOn2bKpOPxyrhNZmcA
UsuFp5A4mHoMqi4LWO0XqCTBzC1r3myx9j3dVg0yJ0LuIvYWUoqOsHI1ywG+ryLO
MfSbpvFgbfU5pn3e61hS++oIpOjmlLuRdu1o/2vHizqcUSfhKx2ccdOUG0c2Opr/
oabL6WpJHRePXbz1jdOPHGVPVH/6OVVsr+L2Ug1Qd8hBLwwbcfGweQ==
=pX05
```

-----END PGP SIGNATURE-----