

[NEWS] Cisco Catalyst 6000, 6500 and Cisco 7600 Series MPLS Packet Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-03/msg00006.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 1 Mar 2007 18:42:23 +0200
-

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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

Cisco Catalyst 6000, 6500 and Cisco 7600 Series MPLS Packet Vulnerability

SUMMARY

Cisco Catalyst 6500 series systems that are running certain versions of Cisco Internetwork Operating System (IOS) are vulnerable to an attack from a Multi Protocol Label Switching (MPLS) packet. Only the systems that are running in Hybrid Mode (Catalyst OS (CatOS) software on the Supervisor Engine and IOS Software on the Multilayer Switch Feature Card (MSFC)) or running with Cisco IOS Software Modularity are affected.

MPLS packets can only be sent from the local network segment.

DETAILS

Affected Products:

Vulnerable Products:

The following products are affected by this vulnerability:

* Cisco Catalyst 6500 systems that run 12.2(18)SXF4 with Cisco IOS Software Modularity are affected.

Images that support Cisco IOS Software Modularity have a "-vz" suffix in their image name.

[NEWS] Cisco Catalyst 6000, 6500 and Cisco 7600 Series MPLS Packet Vulnerability

The following is a conclusive list of all image names that are running with Cisco IOS Software Modularity and are affected by this vulnerability.

- * s72033-adventerprisek9_wan-vz.122-18.SXF4.bin
- * s72033-adviservicesk9_wan-vz.122-18.SXF4.bin
- * s72033-entservicesk9_wan-vz.122-18.SXF4.bin
- * s72033-ipservices_wan-vz.122-18.SXF4.bin
- * s72033-ipservicesk9_wan-vz.122-18.SXF4.bin
- * s72033-ipservicesk9-vz.122-18.SXF4.bin

* Cisco Catalyst 6000, 6500 and Cisco 7600 series systems with an MSFC2 or MSFC3 that run in Hybrid Mode are affected.

In Hybrid Mode, Catalyst OS (CatOS) software runs on the Supervisor Engine and IOS runs on the MSFC. It is different from the Native Mode in which IOS runs both on the Supervisor Engine and MSFC.

This vulnerability affects MSFC2, MSFC2a and MSFC3 that run certain images in Hybrid mode.

In Hybrid Mode, IOS images that run on MSFC start with "c6msfc2", "c6msfc2a" or "c6msfc3". Several image names that run on MSFC in hybrid mode are provided below for reference:

- * c6msfc2a-adventerprisek9_wan-mz.122-18.SXF
- * c6msfc3-jsv-mz.122-14.SX2

Products Confirmed Not Vulnerable:

- * Systems that are running in Native Mode without Cisco IOS Software Modularity are not affected.
- * Systems without an MSFC2, MSFC2a or MSFC3 are not affected.

No other Cisco products are known to be affected by this vulnerability.

Details:

Cisco IOS Software Modularity combines subsystems into individual processes and enhances the Cisco IOS Software memory architecture to provide process-level fault isolation and subsystem "In Service Software Upgrade" (ISSU) capability. These enhancements are delivered in Cisco IOS Software for the Catalyst 6500 Series Supervisor Engine 720 and Supervisor Engine 32. Cisco IOS Software Modularity was first delivered as an option in a Cisco IOS Software Release 12.2(18)SXF4. More information on Modular IOS can be found at the following URL:

http://www.cisco.com/en/US/products/hw/switches/ps708/prod_bulletin0900aecd80313e15.html
http://www.cisco.com/en/US/products/hw/switches/ps708/prod_bulletin0900aecd80313e15.html

Not all 12.2(18)SXF4 images support Modular IOS. Only the images with a "-vz" in the image name support Modular IOS and are affected by this vulnerability. A conclusive list of all affected image names that support

[NEWS] Cisco Catalyst 6000, 6500 and Cisco 7600 Series MPLS Packet Vulnerability

Cisco IOS Software Modularity is provided in the Affected Products section.

In Hybrid Mode, a CatOS image is used as the system software to run the Supervisor Engine on the Catalyst systems. If an MSFC is installed, a separate IOS Software image is used in order to run the MSFC. CatOS provides the Layer 2 (L2) switching functionality. The Cisco IOS on the MSFC provides the Layer 3 (L3) routing functionality. It differs from the Native Mode, in which a single Cisco IOS Software image is used as the system software to run both the Supervisor Engine and MSFC on the Catalyst systems. IOS software that runs on MSFC in Hybrid Mode is also affected by this vulnerability. More information about the differences between Hybrid and Native Modes can be found at the following URL:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a00800c8441.shtml
http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a00800c8441.shtml

MPLS packets received by a Route Processor (MSFC) Layer 3 interface can potentially trigger this vulnerability. The system in question does not need to be configured for MPLS to be vulnerable. MPLS packets can only be sent from the local network segment, limiting the scope of the exploitation.

This issue is documented in bug IDs

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd37415>
CSCsd37415 (registered customers only) and
<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef90002>
CSCef90002 (registered customers only) .

Impact:

Successful exploitation of the vulnerability may result in the reload of the system on systems that are running with Cisco IOS Software Modularity and the reload of MSFC on systems that are running in Hybrid Mode.

Repeated exploitation may lead to a denial of service condition.

Workarounds:

There are no workarounds for this vulnerability.

Additional mitigations that can be deployed on Cisco devices within the network are available in the Cisco Applied Intelligence companion document for this advisory:

<http://www.cisco.com/warp/public/707/cisco-air-20070228-mpls.shtml>

ADDITIONAL INFORMATION

The information has been provided by <mailto:psirt@xxxxxxxx> Cisco Systems Product Security Incident Response Team.

The original article can be found at:

[NEWS] Cisco Catalyst 6000, 6500 and Cisco 7600 Series MPLS Packet Vulnerability

<<http://www.cisco.com/warp/public/707/cisco-sa-20070228-mpls.shtml>>
<http://www.cisco.com/warp/public/707/cisco-sa-20070228-mpls.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@xxxxxxxxxxxxxxxxx
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====
=====

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.