

[NEWS] Cisco Crafted Layer 2 Frame Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-02/0010.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 02/05/04

To: list@securiteam.com

Date: 5 Feb 2004 19:02:32 +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 Crafted Layer 2 Frame Vulnerability

SUMMARY

A layer 2 frame (as defined in the Open System Interconnection Reference Model) that encapsulates a layer 3 packet (IP, IPX, etc.) may cause the specified products to freeze or reset, if the actual length of this frame is inconsistent with the length of the encapsulated layer 3 packet. The vulnerability may be exploited repeatedly causing a denial of service condition.

DETAILS

Vulnerable Systems:

* Cisco 6000/6500/7600 series systems with MSFC2 and a FlexWAN or OSM module

* Cisco 6000/6500/7600 series systems with MSFC2 that are running 12.1(8b)E14

Immune Systems:

* Cisco 6000/6500/7600 series systems with a Supervisor 720

To determine the type of MSFC used on the system, refer to

<<http://www.cisco.com/warp/public/473/96.html>>

<http://www.cisco.com/warp/public/473/96.html>.

Securiteam: [NEWS] Cisco Crafted Layer 2 Frame Vulnerability

A layer 3 packet that is routed by the affected systems may trigger this vulnerability if the packet is encapsulated in a specially crafted layer 2 frame. Crafted packets must be software switched on the vulnerable systems to trigger this vulnerability. The packets that are switched in hardware will not trigger this vulnerability. If the vulnerability is triggered, a denial of service condition could occur. The system can either freeze or reset, and a system that is frozen due to this vulnerability can only be recovered by a system reset.

Although such frames can only be sent from the local network segment, there might be some cases where it is possible to trigger this vulnerability remotely. For remote exploitation, the crafted layer 2 frames need to pass through all the intermediate layer 3 devices between the source and the destination without being clipped. Remote exploitation will not be possible even if only a single layer 3 device on the path from source to destination clips the crafted layer 2 frame.

This vulnerability has been addressed by the Cisco Bug IDs CSCdy15598 and CSCeb56052:

* CSCdy15598 – Affects Cisco 6000/6500/7600 series with an MSFC2 and a FlexWAN or OSM module. The systems that do not have a FlexWAN or OSM will not be affected by this bug.

* CSCeb56052 – Affects Cisco 6000/6500/7600 series with an MSFC2 module. Only 12.1(8b)E14 is affected by this bug, other software versions are not affected. The systems without a FlexWAN or OSM will still be affected by this bug if they are running 12.1(8b)E14.

Workaround

There is no workaround available. The vulnerability can only be mitigated by upgrading to a newer software version.

ADDITIONAL INFORMATION

The original article can be found at:

<<http://www.cisco.com/warp/public/707/cisco-sa-20040203-cat6k.shtml>>
<http://www.cisco.com/warp/public/707/cisco-sa-20040203-cat6k.shtml>.

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

=====

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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

Securiteam: [NEWS] Cisco Crafted Layer 2 Frame Vulnerability

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.