

[NEWS] Cisco Catalyst 6000, 6500 Series and Cisco 7600 Series NAM (Network Analysis Module) Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-03/msg00007.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 1 Mar 2007 18:39:30 +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 Series and Cisco 7600 Series NAM (Network Analysis Module) Vulnerability

SUMMARY

Cisco Catalyst 6000, 6500 series and Cisco 7600 series that have a Network Analysis Module installed are vulnerable to an attack, which could allow an attacker to gain complete control of the system. Only Cisco Catalyst systems that have a NAM on them are affected. This vulnerability affects systems that run Internetwork Operating System (IOS) or Catalyst Operating System (CatOS).

DETAILS

Affected Products:

Vulnerable Products:

Catalyst 6000, 6500 series and Cisco 7600 series that have a NAM installed in them are affected. A system that has a NAM can be identified by the show module command. A NAM will be seen as WS-SVC-NAM-1, WS-SVC-NAM-2 or WS-X6380-NAM in this output.

[NEWS] Cisco Catalyst 6000, 6500 Series and Cisco 7600 Series NAM (Network Analysis Module) Vulnerability

This vulnerability affects systems that run IOS or CatOS.

A sample output for a system that has a NAM-2 on it is provided below:

```
Cat6k#show module
```

```
Mod Ports Card Type Model
```

```
Serial No.
```

```
-----  
-----  
1 2 Catalyst 6000 supervisor 2 (Active) WS-X6K-SUP2-2GE  
SAL06417E23  
3 48 48 port 10/100 mb RJ-45 ethernet WS-X6248-RJ-45  
SAD050108R4  
5 8 8 port 1000mb ethernet WS-X6408-GBIC  
SAD041300CL  
6 8 Network Analysis Module WS-SVC-NAM-2  
SAD093002AM
```

Products Confirmed Not Vulnerable:

- * Catalyst 6000, 6500 and Cisco 7600 series that do not have a NAM are not affected.

- * Network Analysis Modules for Cisco Branch Routers (NM-NAM) are not affected.

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

Details:

NAMs are deployed in Catalyst 6000, 6500 series and Cisco 7600 series to monitor and analyze network traffic by using Remote Monitoring (RMON), RMON2, and other MIBs. More information about NAMs can be found at the following URL:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_module_configuration_guide_chapter09186a008.html
http://www.cisco.com/en/US/products/hw/switches/ps708/products_module_configuration_guide_chapter09186a0080.html

NAMs communicate with the Catalyst system by using the Simple Network Management Protocol (SNMP). By spoofing the SNMP communication between the Catalyst system and the NAM an attacker may obtain complete control of the Catalyst system.

Devices running both Cisco IOS and Cisco CatOS are affected by this vulnerability. This vulnerability is introduced in CatOS at 7.6(15) and 8.5(1). Older CatOS images are not vulnerable.

This issue is documented in bug IDs

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd75273>>

CSCsd75273 (registered customers only) ,

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse52951>>

CSCse52951 (registered customers only) for IOS and

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse39848>>

[NEWS] Cisco Catalyst 6000, 6500 Series and Cisco 7600 Series NAM (Network Analysis Module) Vulnerability

[NEWS] Cisco Catalyst 6000, 6500 Series and Cisco 7600 Series NAM (Network Analysis Module) Vulnerability

CSCc39848 (registered customers only) for CatOS.

Impact:

By successfully exploiting this vulnerability, an attacker may gain complete control of the device.

Workarounds:

No workarounds exist for this vulnerability.

This vulnerability requires an attacker to spoof SNMP packets from the IP address of the NAM. Filtering SNMP traffic to an affected device can be used as a mitigation. Filtering SNMP traffic needs to be done on systems that are deployed in front of an affected device, since it is ineffective to filter against such spoofed packets on the device itself.

Anti-spoofing measures and infrastructure access-lists can also be deployed at your network edge as a potential mitigation technique. Refer to <<http://www.cisco.com/warp/public/707/iacl.html>> <http://www.cisco.com/warp/public/707/iacl.html> for examples on how to apply ACLs on Cisco routers for infrastructure protection.

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

<<http://www.cisco.com/warp/public/707/cisco-sa-20070228-nam.shtml>>
<http://www.cisco.com/warp/public/707/cisco-sa-20070228-nam.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@xxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxx

=====
=====

DISCLAIMER:

[NEWS] Cisco Catalyst 6000, 6500 Series and Cisco 7600 Series NAM (Network Analysis Module) Vulnerability

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.