

# Cisco Security Advisory: Cisco Catalyst 6000, 6500 Series and Cisco 7600 Series NAM (Network Analysis Module) Vulnerability

Advisory ID: cisco-sa-20070228-nam

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

## Revision 1.1

Last Updated 2007 March 15 1732 UTC (GMT)

For Public Release 2007 February 28 1600 UTC (GMT)

---

Please provide your [feedback](#) on this document.

---

## Contents

- [Summary](#)
- [Affected Products](#)
- [Details](#)
- [Impact](#)
- [Software Version and Fixes](#)
- [Workarounds](#)
- [Obtaining Fixed Software](#)
- [Exploitation and Public Announcements](#)
- [Status of this Notice: FINAL](#)
- [Distribution](#)
- [Revision History](#)
- [Cisco Security Procedures](#)

---

## 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).

Cisco has made free software available to address this vulnerability for affected customers.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070228-nam.shtml>.

[\[Expand all sections\]](#) [\[Collapse all sections\]](#)

## ☐ 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.

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
-----
1 2 Catalyst 6000 supervisor 2 (Active) WS-X6K-SUP2-2GE SAL06
3 48 48 port 10/100 mb RJ-45 ethernet WS-X6248-RJ-45 SAD05
5 8 8 port 1000mb ethernet WS-X6408-GBIC SAD04
6 8 Network Analysis Module WS-SVC-NAM-2 SAD09
```

### ☐ 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.

[Top of the section](#) [Close Section](#)

## ☐ 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\\_ch](http://www.cisco.com/en/US/products/hw/switches/ps708/products_module_configuration_guide_ch)

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 [CSCsd75273](#) ([registered](#) customers only) , [CSCse52951](#) ([registered](#) customers only) for IOS and [CSCse39848](#) ([registered](#) customers only) for CatOS.

## Vulnerability Scoring Details

Cisco is providing scores for the vulnerabilities in this advisory based on the Common Vulnerability Scoring System (CVSS). Cisco will provide a base and temporal score. Customers can then compute environmental scores to assist in determining the impact of the vulnerability in individual networks.

Cisco PSIRT will set the bias in all cases to normal. Customers are encouraged to apply the bias parameter when determining the environmental impact of a particular vulnerability.

CVSS is a standards-based scoring method that conveys vulnerability severity and helps determine urgency and priority of response.

Cisco has provided an FAQ to answer additional questions regarding CVSS at <http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html>.

Cisco has also provided a CVSS calculator to help compute the environmental impact for individual networks at <http://intellishield.cisco.com/security/alertmanager/cvss>

<a href="#">CSCsd75273 - Cat6k NAM vulnerability ( <a href="#">registered</a> customers only) <a href="#">Calculate the environmental score of CSCsd75273</a> ↗</a>						
CVSS Base Score - <b>10</b>						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Not Required	Complete	Complete	Complete	Normal
CVSS Temporal Score - <b>8.3</b>						
Exploitability		Remediation Level		Report Confidence		
Functional		Official Fix		Confirmed		

<a href="#">CSCse52951 - Catk NAM vulnerability, additional protection ( <a href="#">registered</a> customers only) <a href="#">Calculate the environmental score of CSCse52951</a> ↗</a>						
CVSS Base Score - <b>10</b>						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Not Required	Complete	Complete	Complete	Normal
CVSS Temporal Score - <b>8.3</b>						
Exploitability		Remediation Level		Report Confidence		
Functional		Official Fix		Confirmed		

<a href="#">CSCse39848 - Cat6k NAM vulnerability in CatOS ( registered customers only)</a> <a href="#">Calculate the environmental score of CSCse39848</a>						
CVSS Base Score - <b>10</b>						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Not Required	Complete	Complete	Complete	Normal
CVSS Temporal Score - <b>8.3</b>						
Exploitability		Remediation Level		Report Confidence		
Functional		Official Fix		Confirmed		

[Top of the section](#)   [Close Section](#)

## Impact

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

[Top of the section](#)   [Close Section](#)

## Software Version and Fixes

When considering software upgrades, also consult <http://www.cisco.com/go/psirt> and any subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, contact the Cisco Technical Assistance Center ("TAC") or your contracted maintenance provider for assistance.

Each row of the Cisco IOS software table (below) describes a release train and the platforms or products for which it is intended. If a given release train is vulnerable, then the earliest possible releases that contain the fix (the "First Fixed Release") and the anticipated date of availability for each are listed in the "Rebuild" and "Maintenance" columns. A device running a release in the given train that is earlier than the release in a specific column (less than the First Fixed Release) is known to be vulnerable. The release should be upgraded at least to the indicated release or a later version (greater than or equal to the First Fixed Release label).

For more information on the terms "Rebuild" and "Maintenance," consult the following URL: <http://www.cisco.com/warp/public/620/1.html>.

Major Release	Availability of Repaired Releases	
Affected 12.1-Based Release	Rebuild	Maintenance
12.1E	12.1(26)E8	

	12.1(27b)E1	
12.1EX	12.1(12c)EX	12.1(13)EX
<b>Affected 12.2- Based Release</b>	<b>Rebuild</b>	<b>Maintenance</b>
12.2EU	Vulnerable; migrate to 12.2(25) EWA7 or later	
12.2EW	Vulnerable; migrate to 12.2(25) EWA7 or later	
12.2EWA		12.2(25)EWA7
12.2IXA	Vulnerable; migrate to 12.2(18) IXB2 or later	
12.2IXB	12.2(18)IXB2	
12.2S	12.2(14)S3	
	12.2(18)S5	12.2(20)S
12.2SG	12.2(25)SG1	
12.2SGA	12.2(31)SGA1	
12.2SRA	12.2(33)SRA2	
12.2SX	Vulnerable; migrate to 12.2(18) SXD7a or later	
12.2SXA	Vulnerable; migrate to 12.2(18) SXD7a or later	
12.2SXB	Vulnerable; migrate to 12.2(18) SXD7a or later	
12.2SXD	12.2(18) SXD7a	
12.2SXE	12.2(18) SXE6a	
12.2SXF	12.2(18)SXF5	
12.2SY	Vulnerable; migrate to 12.2(18) SXD7a or later	
12.2ZA	Vulnerable; migrate to 12.2(18) SXD7a or later	
12.2ZU	12.2(18)ZU1	

CatOS Release	Availability of Fixed Releases	
	Interim	Maintenance
5.x	Not vulnerable	

6.x	Not vulnerable	
7.6(1) through 7.6(14)	Not vulnerable	
7.6(15) through 7.6(19)	7.6(19.2)	7.6(20) Available 2007-Mar-21
8.5(1) through 8.5(5)	8.5(5.3)	8.5(6)
8.6(x)	Not vulnerable	

[Top of the section](#)   [Close Section](#)

## 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> 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 Mitigation Bulletin companion document for this advisory: <http://www.cisco.com/warp/public/707/cisco-amb-20070228-nam.shtml>

[Top of the section](#)   [Close Section](#)

## Obtaining Fixed Software

Cisco will make free software available to address this vulnerability for affected customers. This advisory will be updated as fixed software becomes available. Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

Customers may only install and expect support for the feature sets they have purchased. By installing, downloading, accessing or otherwise using such software upgrades, customers agree to be bound by the terms of Cisco's software license terms found at <http://www.cisco.com/public/sw-license-agreement.html>, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software upgrades.

[Top of the section](#)   [Close Section](#)

## ☐ Customers with Service Contracts

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's worldwide website at <http://www.cisco.com>.

[Top of the section](#)   [Close Section](#)

## ☐ Customers using Third Party Support Organizations

Customers whose Cisco products are provided or maintained through prior or existing agreement with third-party support organizations such as Cisco Partners, authorized resellers, or service providers should contact that support organization for guidance and assistance with the appropriate course of action in regards to this advisory.

The effectiveness of any workaround or fix is dependent on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. Due to the variety of affected products and releases, customers should consult with their service provider or support organization to ensure any applied workaround or fix is the most appropriate for use in the intended network before it is deployed.

[Top of the section](#)   [Close Section](#)

## ☐ Customers without Service Contracts

Customers who purchase direct from Cisco but who do not hold a Cisco service contract and customers who purchase through third-party vendors but are unsuccessful at obtaining fixed software through their point of sale should get their upgrades by contacting the Cisco Technical Assistance Center (TAC). TAC contacts are as follows.

- +1 800 553 2447 (toll free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)
- e-mail: [tac@cisco.com](mailto:tac@cisco.com)

Have your product serial number available and give the URL of this notice as evidence of your entitlement to a free upgrade. Free upgrades for non-contract customers must be requested through the TAC.

Refer to <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> for additional TAC contact information, including special localized telephone numbers and instructions and e-mail addresses for use in various languages.

[Top of the section](#)   [Close Section](#)

## ☐ Exploitation and Public Announcements

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerability described in this advisory.

This vulnerability was found internally.

[Top of the section](#)   [Close Section](#)

## ☐ **Status of this Notice: FINAL**

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

A stand-alone copy or Paraphrase of the text of this document that omits the distribution URL in the following section is an uncontrolled copy, and may lack important information or contain factual errors.

[Top of the section](#)   [Close Section](#)

## ☐ **Distribution**

This advisory is posted on Cisco's worldwide website at:

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

In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key and is posted to the following e-mail and Usenet news recipients.

- [cust-security-announce@cisco.com](mailto:cust-security-announce@cisco.com)
- [first-teams@first.org](mailto:first-teams@first.org)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [vulnwatch@vulnwatch.org](mailto:vulnwatch@vulnwatch.org)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [cisco-nsp@puck.nether.net](mailto:cisco-nsp@puck.nether.net)
- [full-disclosure@lists.grok.org.uk](mailto:full-disclosure@lists.grok.org.uk)
- [comp.dcom.sys.cisco@newsgate.cisco.com](mailto:comp.dcom.sys.cisco@newsgate.cisco.com)

Future updates of this advisory, if any, will be placed on Cisco's worldwide website, but may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the above URL for any updates.

[Top of the section](#)   [Close Section](#)

## ☐ **Revision History**

Revision 1.1	2007-March- 15	Updated the availability date of CatOS release 7.6(20)

Revision 1.0	2007- February-28	Initial public release.
-----------------	----------------------	-------------------------

[Top of the section](#)   [Close Section](#)

## ☐ Cisco Security Procedures

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html). This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

[Top of the section](#)   [Close Section](#)

---

<a href="#">Home</a>	<a href="#">How to Buy</a>	<a href="#">Login</a>	<a href="#">Profile</a>	<a href="#">Feedback</a>	<a href="#">Site Map</a>	<a href="#">Help</a>
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

All contents are Copyright © 2006-2007 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).