

Cisco Security Response: PHP HTML Entity Encoder Heap Overflow Vulnerability in Multiple Web-Based Management Interfaces

<http://www.cisco.com/warp/public/707/cisco-sr-20070425-http.shtml>

Revision 1.0

Last Updated 2007 April 25 1600 UTC (GMT)

For Public Release 2007 April 25 1600 UTC (GMT)

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

Contents

[Cisco Response](#)
[Additional Information](#)
[Revision History](#)
[Cisco Security Procedures](#)

Cisco Response

This is a response to a Hardened-PHP Project advisory posted on November 3, 2006, entitled "PHP HTML Entity Encoder Heap Overflow Vulnerability." This advisory is available at the following link: http://www.hardened-php.net/advisory_132006.138.html.

Several Cisco devices leverage PHP HTML support and are affected by the described vulnerability. The affected devices are listed below.

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 Mitigation Bulletin companion document for this advisory at the following link: <http://www.cisco.com/warp/public/707/cisco-amb-20070425-http.shtml>.

This Cisco Security Response is posted at the following link:
<http://www.cisco.com/warp/public/707/cisco-sr-20070425-http.shtml>.

Additional Information

The following products are affected by this vulnerability:

- Network Analysis Modules (NAM) for Cisco 6500 switch, Cisco 7600 router and Branch Routers
 - Vulnerability is addressed via Cisco bug ID: [CSCsg76978](#) ([registered](#) customers only) .
 - There are three different models of NAM for the Catalyst 6000, 6500 series switches and Cisco 7600 series router; the WS-SVC-NAM-1, WS-SVC-NAM-2 or WS-X6380-NAM . All three models are affected by this vulnerability.
 - Network Analysis Modules for Cisco Branch Routers (NM-NAM) are affected.
 - Access to the pages that contain PHP code requires previous authentication.
 - Devices running software versions 3.5(1a) and earlier are potentially affected by this vulnerability.

Software Fixes

- Software version 3.5(1b) and later contain fixed PHP code.
 - Software version 3.6 and later contain fixed PHP code.
 - There is no software fix for the WS-X6380-NAM.
 - The software is available for download from <http://www.cisco.com/tacpage/sw-center/netmgmt/nam.shtml> ([registered](#) customers only) .
- CiscoWorks Wireless LAN Solution Engine (WLSE) and CiscoWorks Wireless LAN Solution Engine Express (WLSX)
 - Vulnerability is being addressed via Cisco bug ID: [CSCsg92199](#) ([registered](#) customers only) .
 - There are no PHP pages that are reachable from a user session. The WLSE/WLSX have a few PHP scripts that are run on the backend, which are not exploitable.

Software Fixes

- Currently no fixed version of WLSE/WLSX software exists.
 - The version of PHP code within the WLSE/WLSX will be upgraded to a fixed release via the above mentioned Cisco bug ID.
 - This response will be updated once the DDTS is resolved.
- Cisco Unified Application Environment
 - Vulnerability is addressed via Cisco bug ID: [CSCsg92204](#) ([registered](#) customers only) .
 - Access to the pages that contain the PHP code requires previous authentication.
 - Devices running software versions 2.3.x and earlier are potentially affected by this vulnerability.

Software Fixes

- Software version 2.4, due for release in May 2007, will contain the fixed PHP code.
- Hosting Solution Engine/Hosting Solution Software
 - Vulnerability is addressed via Cisco bug ID: [CSCsg92193](#) ([registered](#) customers only) .
 - All versions of software without the integrated patch installed are affected by this vulnerability.
 - Access to the pages that contain PHP code requires previous authentication.

Software Fixes

- A software patch has been issued for Hosting Solution Engine/Hosting Solution Software 1.9 on March 21, 2007.
- The patch is called 'HSE-1.9u2.zip' and is available for download from <http://www.cisco.com/cgi-bin/tablebuild.pl/1105-host-sol> ([registered](#) customers only) .

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

Workarounds

No workarounds exist for this vulnerability.

A best practice is to configure IP source restriction to valid source IP addresses of administrative clients that may access the affected devices. Administrators should restrict access to the web interface to only trusted client IP addresses or subnets.

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 at the following link:
<http://www.cisco.com/warp/public/707/cisco-amb-20070425-http.shtml>

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.

Revision History

| | | |
|--------------|---------------|------------------------|
| Revision 1.0 | 2007-April-25 | Initial public release |
|--------------|---------------|------------------------|

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. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

Help us help you.

Please rate this document.

- Excellent
 Good

- Average
- Fair
- Poor

This document solved my problem.

- Yes
- No
- Just browsing

Suggestions for improvement:

(256 character limit)

| | | | | | | |
|----------------------|----------------------------|-----------------------|-------------------------|--------------------------|--------------------------|----------------------|
| Home | How to Buy | Login | Profile | Feedback | Site Map | Help |
|----------------------|----------------------------|-----------------------|-------------------------|--------------------------|--------------------------|----------------------|