

[Solutions](#) [Products](#) [Ordering](#) [Support](#) [Partners](#) [Training](#) [Corporate](#)[Security Responses](#)

Cisco Security Response: VTY Authentication Bypass Vulnerability

<http://www.cisco.com/warp/public/707/cisco-sr-20070829-vty.shtml>

Revision 1.2

Last Updated 2007 September 07 1730 UTC (GMT)

For Public Release 2007 August 29 1800 UTC (GMT)

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

Contents

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

Cisco Response

This is the Cisco PSIRT response to the NileSOFT Security Advisory entitled "Bypass Authentication Vulnerability on Cisco Catalyst 3750 12.2(25)" posted on August 29th, 2007, at 1800 UTC (GMT).

The original advisory was posted to a Korean website.

This vulnerability was previously discovered and reported to Cisco by a customer in April 2005, and the contents of the Cisco Bug ID have been available on Cisco.com since April 2005. This is a platform independent vulnerability, and is not limited to just the Catalyst 3750 device.

This vulnerability is documented in Cisco Bug ID [CSCsa91175](#) ([registered](#) customers only) .

This Cisco Security Response is posted at the following link:

<http://www.cisco.com/warp/public/707/cisco-sr-20070829-vty.shtml>.

Additional Information

The contents of the Cisco Bug ID [CSCsa91175](#) ([registered](#) customers only) release note enclosure is shown below:

Symptom

If Authentication, Authorization and Accounting (AAA) is not enabled on a device and any configuration is entered under the VTY/AUX or CONSOLE line (except the **login** command), the command "**no login**" will appear under the VTY lines.

Conditions

This symptom will only occur if AAA is not enabled on the device and any configuration changes are made according to the Symptom description above. Although the command "**no login**" will appear in the configuration, the device is not vulnerable until the running-configuration is saved to NVRAM and the device is reloaded.

Cisco IOS® Software Releases within 12.2 E, F, and S release trains are affected if Cisco Bug ID [CSCsa91175](#) ([registered](#) customers only) is not integrated. Cisco recommends checking the device configuration to confirm that under the VTY lines the command "**no login**" is not present, unless this is the desired configuration. Provided below is a list of affected trains and the first fixed release.

Affected Release:	First Fixed Releases:
12.2E based trains EW EWA EU EX EY	Vulnerable; apply workaround Vulnerable; apply workaround Vulnerable; apply workaround Fixed in 12.2(35)EX Fixed in 12.2(37)EY
12.2F based trains FX FY FZ	Vulnerable; apply workaround Vulnerable; apply workaround Vulnerable; apply workaround
12.2S based trains S SB SBC SE SEA SEB SEC SED SEE SEF SEG SG SV SW SXD SXE SZ	Vulnerable; apply workaround Fixed in 12.2(31)SB Vulnerable; apply workaround Fixed in 12.2(35)SE Vulnerable; apply workaround Vulnerable; apply workaround Vulnerable; apply workaround Vulnerable; apply workaround Vulnerable; apply workaround Vulnerable; apply workaround Vulnerable; apply workaround Fixed in 12.2(31)SG Vulnerable; apply workaround Vulnerable; apply workaround Vulnerable; apply workaround Fixed in 12.2(18)SXE4 and later Vulnerable; apply workaround

No other Cisco IOS release trains are known to be affected by this vulnerability.

For more information on the terms "releases" and "trains," consult the following URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_white_paper09186a008018305e.sht

In order to check the device configuration, log in to the device and enter the privileged command "**show running-config**". Confirm under the VTY lines that the command "**no login**" is not present, unless this is the desired configuration.

For further information on the "**login**" command please reference:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/tersv_r/ter_11g.htm#wp9982

An example of a device that will allow remote terminal access without a password prompt is shown below:

```
Device#show running-config
<lines removed>
line VTY 0 4
  no login
<lines removed>
```

Workaround

Configuring the VTY lines with "**login**" will ensure that any remote access is prompted for a password first.

Cisco recommends for customers to migrate to SSH as a best practice - where available and practical.

Note: If configured for AAA, please consult the AAA configuration guides for additional commands that are used with the **login** command.

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 1.2	2007-September-07	Affected Releases table updated to include information for 12.2S based trains for SEB and SEC
Revision 1.1	2007-August-30	Cisco Response section updated to indicate that the platform is not limited to just the Catalyst 3750 device

Revision 1.0	2007- August-29	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](#)

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