

# Cisco Security Response: AAA Command Authorization by-pass

Document ID: 68840

<http://www.cisco.com/warp/public/707/cisco-sr-20060125-aaatcl.shtml>

## Revision 2.0

**Last Updated** 2006 March 01 1600 UTC (GMT)

**For Public Release** 2006 January 25 1600 UTC (GMT)

---

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

---

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

---

## Cisco Response

This is an update to the original Cisco Vendor Response posted on 2006 January 25 16:00 UTC at:  
<http://www.cisco.com/warp/public/707/cisco-response-20060125-aaatcl.shtml>.

Since the original posting, it has been discovered that some versions of Cisco IOS originally documented as fixed were still affected by this vulnerability. This new issue is being tracked with Cisco Bug ID [CSCsd28570](#) ([registered](#) customers only) . An updated Cisco IOS "Software versions and fixes" table is within. All other relevant information remains unaltered.

A vulnerability exists within Cisco Internetwork Operating System (IOS) Authentication, Authorization, and Accounting (AAA) command authorization feature, where command authorization checks are not performed on commands executed from the Tool Command Language (Tcl) exec shell. This may allow authenticated users to bypass command authorization checks in some configurations resulting in unauthorized privilege escalation.

Devices not running AAA command authorization feature, or do not support Tcl functionality are not affected by this vulnerability.

We would like to thank Nicolas Fischbach, Senior Manager, Network Engineering Security of COLT Telecom, for reporting this issue to Cisco Systems.

We greatly appreciate the opportunity to work with researchers on security vulnerabilities, and welcome the opportunity to review and assist in product reports.

## Additional Information

## Details

Devices that are running AAA command authorization feature and the IOS has support for the Tcl functionality, may be affected by this vulnerability.

A device that has Tcl functionality within IOS, will accept the command **tclsh** and provide a command-line interface (CLI) prompt back with (tcl) in the CLI prompt. Example:

```
router#tclsh
router(tcl)#
```

If the device does not support Tcl functionality, either an error message or different output will be displayed.

The (tcl) text within the CLI prompt indicates that the user is within the Tcl Shell mode.

A system configured for AAA command authorization will have a command line in **show running-configuration** output, which is similar to the following:

```
aaa authorization commands <privilege-level> <default|list-name> <group [group-name]>
tacacs+ [additional methods]
```

Example:

```
aaa authorization commands 15 default group tacacs+ none
```

Devices impacted by this vulnerability, will allow users to execute any IOS EXEC command at the users authenticated privilege level from within the Tcl shell mode. This vulnerability is documented in the following bug IDs:

- [CSCeh73049](#) ([registered](#) customers only) — tclsh mode bypasses AAA command authorization check
- [CSCsd28570](#) ([registered](#) customers only) — tclsh bypass of AAA authorization commands

A separate issue, documented below, exists that exacerbates this vulnerability. An authenticated user may be placed into Tcl Shell mode automatically (without the evidence of the (tcl) within the router prompt), without any intermediate step of manually entering into Tcl Shell mode via the **tclsh** command, only if a previous user goes into Tcl Shell mode and terminates the session before leaving the Tcl Shell mode.

If a privileged user initiates a Tcl Shell and exits the Tcl Shell mode without issuing the Tcl Shell command **tclquit** then the Tcl Shell process will remain active and attached to the corresponding virtual type terminal VTY or teletypewriter (TTY – line). The next authenticated user that accesses the device over the same line will have access to the Tcl Shell process, and combined with [CSCeh73049](#) ([registered](#) customers only) or [CSCsd28570](#) ([registered](#) customers only) may bypass AAA command. This issue is documented in the following bug ID:

- [CSCef77770](#) ([registered](#) customers only) — Type ctrl-c or ctrl-z causes tclsh prompt to disappear

This separate issue is present only in the versions of IOS listed below:

- 12.3T based trains
- 12.4 based trains
- 12.2(25)S and onward trains

## Vulnerable Products

- All Cisco products that are running Cisco IOS and:
  - Have AAA command authorization feature enabled
  - The IOS has support for the Tcl functionality
  - IOS Version 12.0T or later

## Products Confirmed Not Vulnerable

- Products that are not running Cisco IOS are not affected.
- Products running Cisco IOS versions 12.0 Mainline or earlier are not affected.
- Products running Cisco IOS versions 12.0S are not affected.
- Products that are running Cisco IOS are not affected unless they are configured for AAA command authorization, and support Tcl functionality.
- Products that are running Cisco IOS XR are not affected.

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

## Software Versions and Fixes

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).

Major Release	Availability of Repaired Releases	
<b>Affected 12.0–Based Release</b>	<b>Rebuild</b>	<b>Maintenance</b>
12.0T	Vulnerable; migrate to 12.2(32) or later	
12.0XH	Vulnerable; migrate to 12.2(32) or later	
12.0XK	Vulnerable; migrate to 12.2(32) or later	
12.0XL	Vulnerable; migrate to 12.2(32) or later	
12.0XN	Vulnerable; migrate to 12.2(32) or later	
12.0XR	Vulnerable; migrate to 12.2(32) or later	
<b>Affected 12.1–Based Release</b>	<b>Rebuild</b>	<b>Maintenance</b>
12.1	Vulnerable; migrate to 12.2(32) or later	
12.1AA	Vulnerable; migrate to 12.2(32) or later	
12.1E	12.1(26)E5	
12.1EC	Vulnerable; migrate to 12.3BC or later	
12.1EZ	Vulnerable; migrate to 12.1(26)E5 or later	
12.1GA	Vulnerable; migrate to 12.2(32) or later	

12.1GB	Vulnerable; migrate to 12.2(32) or later	
12.1T	Vulnerable; migrate to 12.2(32) or later	
12.1XA	Vulnerable; migrate to 12.2(32) or later	
12.1XE	Vulnerable; migrate to 12.2(32) or later	
12.1XH	Vulnerable; migrate to 12.2(32) or later	
12.1XI	Vulnerable; migrate to 12.2(32) or later	
12.1XJ	Vulnerable; migrate to 12.3(16) or later	
12.1XL	Vulnerable; migrate to 12.3(16) or later	
12.1XM	Vulnerable; migrate to 12.3(16) or later	
12.1XP	Vulnerable; migrate to 12.3(16) or later	
12.1XQ	Vulnerable; migrate to 12.3(16) or later	
12.1XS	Vulnerable; migrate to 12.2(32) or later	
12.1XT	Vulnerable; migrate to 12.3(16) or later	
12.1XU	Vulnerable; migrate to 12.3(16) or later	
12.1XV	Vulnerable; migrate to 12.3(16) or later	
12.1XW	Vulnerable; migrate to 12.2(32) or later	
12.1XY	Vulnerable; migrate to 12.2(32) or later	
12.1XZ	Vulnerable; migrate to 12.2(32) or later	
12.1YA	Vulnerable; migrate to 12.3(16) or later	
12.1YB	Vulnerable; migrate to 12.3(16) or later	
12.1YD	Vulnerable; migrate to 12.3(16) or later	
12.1YE	Vulnerable; migrate to 12.3(16) or later	
12.1YF	Vulnerable; migrate to 12.3(16) or later	
12.1YH	Vulnerable; migrate to 12.3(16) or later	
12.1YI	Vulnerable; migrate to 12.3(16) or later	
<b>Affected 12.2–Based Release</b>	<b>Rebuild</b>	<b>Maintenance</b>
12.2		12.2(32)
12.2B	Vulnerable; migrate to 12.3(14)T7, available 3–April–2006	
12.2BW	Vulnerable; migrate to 12.3(16) or later	
12.2BY	Vulnerable; migrate to 12.3(14)T7, available 3–April–2006	
12.2DD	Vulnerable; migrate to 12.3(14)T7, available 3–April–2006	
12.2DX	Vulnerable; migrate to 12.3(14)T7, available 3–April–2006	

12.2MX	Vulnerable; migrate to 12.3(14)T7, available 3–April–2006	
12.2S	12.2(14)S16	
	12.2(18)S11	
	12.2(25)S6	
	12.2(30)S is vulnerable; contact TAC	
12.2SU	Vulnerable; migrate to 12.3(14)T7, available 3–April–2006	
12.2SW	12.2(25)SW5	
12.2SXB	12.2(17d)SXB9	
12.2SXD	12.2(18)SXD6	
12.2SXE	12.2(18)SXE3	
12.2SXF	Vulnerable; migrate to 12.2(18)SXF4, available 29–May–2006	
12.2SZ	Vulnerable; migrate to 12.2(25)S6 or later	
12.2T	Vulnerable; migrate to 12.3(16) or later	
12.2XA	Vulnerable; migrate to 12.3(16) or later	
12.2XB	Vulnerable; migrate to 12.3(16) or later	
12.2XC	Vulnerable; migrate to 12.3(14)T7, available 3–April–2006	
12.2XD	Vulnerable; migrate to 12.3(16) or later	
12.2XG	Vulnerable; migrate to 12.3(16) or later	
12.2XH	Vulnerable; migrate to 12.3(16) or later	
12.2XJ	Vulnerable; migrate to 12.3(16) or later	
12.2XK	Vulnerable; migrate to 12.3(16) or later	
12.2XL	Vulnerable; migrate to 12.3(16) or later	
12.2XM	Vulnerable; migrate to 12.3(16) or later	
12.2XN	Vulnerable; migrate to 12.3(16) or later	
12.2XQ	Vulnerable; migrate to 12.3(16) or later	
12.2XS	Vulnerable; migrate to 12.3(16) or later	
12.2XT	Vulnerable; migrate to 12.3(16) or later	
12.2XU	Vulnerable; migrate to 12.3(16) or later	
12.2XV	Vulnerable; migrate to 12.3(16) or later	
12.2XW	Vulnerable; migrate to 12.3(16) or later	
12.2YB	Vulnerable; migrate to 12.3(16) or later	
12.2YC	Vulnerable; migrate to 12.3(16) or later	
12.2YD	Vulnerable; migrate to 12.3(14)T7, available 3–April–2006	

12.2YE	<del>Vulnerable; migrate to 12.2(25)S6 or later</del>	
12.2YH	<del>Vulnerable; migrate to 12.3(16) or later</del>	
12.2YK	Vulnerable; migrate to 12.3(14)T7, available 3–April–2006	
12.2YL	Vulnerable; migrate to 12.3(14)T7, available 3–April–2006	
12.2YM	Vulnerable; migrate to 12.3(14)T7, available 3–April–2006	
12.2YN	Vulnerable; migrate to 12.3(14)T7, available 3–April–2006	
12.2YT	<del>Vulnerable; migrate to 12.3(16) or later</del>	
12.2YU	Vulnerable; migrate to 12.3(14)T7, available 3–April–2006	
12.2YW	Vulnerable; migrate to 12.3(14)T7, available 3–April–2006	
12.2YX	Vulnerable; migrate to 12.3(14)T7, available 3–April–2006	
12.2YY	Vulnerable; migrate to 12.3(14)T7, available 3–April–2006	
12.2YZ	<del>Vulnerable; migrate to 12.2(25)S6 or later</del>	
12.2ZB	Vulnerable; migrate to 12.3(14)T7, available 3–April–2006	
12.2ZC	Vulnerable; migrate to 12.3(14)T7, available 3–April–2006	
12.2ZD	<del>Vulnerable; contact TAC</del>	
12.2ZE	<del>Vulnerable; migrate to 12.3(16) or later</del>	
12.2ZF	Vulnerable; migrate to 12.3(14)T7, available 3–April–2006	
12.2ZH	<del>Vulnerable; contact TAC</del>	
12.2ZJ	Vulnerable; migrate to 12.3(14)T7, available 3–April–2006	
12.2ZL	<del>Vulnerable; contact TAC</del>	
12.2ZN	Vulnerable; migrate to 12.3(14)T7, available 3–April–2006	
12.2ZP	Vulnerable; migrate to 12.3(14)T7, available 3–April–2006	
<b>Affected 12.3–Based Release</b>	<b>Rebuild</b>	<b>Maintenance</b>
12.3		12.3(16)
12.3B	Vulnerable; migrate to 12.3(14)T7, available 3–April–2006	

12.3T	12.3(11)T10; available 13–March–2006	
	12.3(14)T7; available 3–April–2006	
12.3XA	Vulnerable; contact TAC	
12.3XB	Vulnerable; migrate to 12.3(14)T7, available 3–April–2006	
12.3XD	Vulnerable; migrate to 12.3(14)T7, available 3–April–2006	
12.3XE	Vulnerable; contact TAC	
12.3XF	Vulnerable; migrate to 12.3(14)T7, available 3–April–2006	
12.3XG	Vulnerable; contact TAC	
12.3XH	Vulnerable; migrate to 12.3(14)T7, available 3–April–2006	
12.3XI	12.3(7)XI7	
12.3XJ	Vulnerable; contact TAC	
12.3XK	Vulnerable; contact TAC	
12.3XM	Vulnerable; migrate to 12.3(14)T7, available 3–April–2006	
12.3XQ	Vulnerable; migrate to 12.4(7), available 14–March–2006	
12.3XR	Vulnerable; contact TAC	
12.3XW	Vulnerable; contact TAC	
12.3XY	Vulnerable; migrate to 12.3(14)T7, available 3–April–2006	
12.3YA	C828: Vulnerable; migrate to 12.4(7), available 14–March–2006	
	SOHO9x, C82x: Vulnerable; contact TAC	
12.3YF	Vulnerable; contact TAC	
12.3YG	Vulnerable; contact TAC	
12.3YH	Vulnerable; contact TAC	
12.3YI	Vulnerable; contact TAC	
12.3YJ	Vulnerable; contact TAC	
12.3YK	Vulnerable; contact TAC	
12.3YM	12.3(14)YM6; available 26–March–2006	
12.3YQ	Vulnerable; contact TAC	
12.3YS	Vulnerable; contact TAC	

12.3YT	Vulnerable; contact TAC	
12.3YU	Vulnerable; contact TAC	
12.3YX	Vulnerable; contact TAC	
<b>Affected 12.4–Based Release</b>	<b>Rebuild</b>	<b>Maintenance</b>
12.4	12.4(3d); available 21–March–2006	
		12.4(7); available 14–March–2006
12.4MR	Vulnerable; contact TAC	
12.4T	12.4(2)T4; available 20–March–2006	
	12.4(4)T2; available 3–April–2006	
		12.4(6)T
12.4XA	Vulnerable; contact TAC	
12.4XB	Vulnerable; contact TAC	

## Obtaining Fixed Software

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

## 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>.

## 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.

## 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.

## Workarounds

The effectiveness of any workaround 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 is the most appropriate for use in the intended network before it is deployed.

### AAA configuration command checks

Adding IOS configuration command authorization checking with the global configuration command **aaa authorization config-commands** forces AAA command authorization to occur within Tcl Shell mode.



**Caution:** By enabling IOS configuration command authorization all commands within EXEC configuration mode will be subject to command authorization checks.

For further information on AAA authorization config-commands please consult:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/secure/sec\\_alg.htm#wp1086510](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/secure/sec_alg.htm#wp1086510).

### Deny tclsh IOS command within TACACS+ user profile

By ensuring that all user profiles defined within TACACS+ do not have permission to execute the IOS EXEC command **tclsh** an administrator can prevent users from gaining additional command privilege escalation. Seek your vendor's TACACS+ server configuration guides to ensure this is set correctly.



**Caution:** This will only be a valid workaround if all users who may access the device do not have access to **tclsh** command. A single user who does have access to execute **tclsh** and does not exit as per the procedure described above, may unknowingly leave a Tcl Shell process running on one of the VTYS.

### Role Based CLI Views

The Role-Based CLI Access feature allows the network administrator to define "views," which are a set of operational commands and configuration capabilities that provide selective or partial access to Cisco IOS EXEC and configuration (Config) mode commands. Views restrict user access to Cisco IOS command-line interface (CLI) and configuration information; that is, a view can define what commands are accepted and what configuration information is visible. Thus, network administrators can exercise better control over access to Cisco networking devices.

For further information on CLI-Views:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hsec\\_c/part30/hclivws.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hsec_c/part30/hclivws.htm).

## Further Information

Cisco IOS introduced the ability to support Tool Command Language (Tcl) version 7.0 commands as part of Cisco IOS Interactive Voice Response feature in Cisco IOS version 12.0(6)T and later. See

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_serv/vapp\\_dev/tclivrpg.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/vapp_dev/tclivrpg.htm) for further information.

The Cisco IOS Scripting with Tcl feature provides the ability to run Tool Command Language (Tcl) version 8.3.4 commands and was introduced from Cisco IOS version 12.3(2)T. See

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t\\_2/gt\\_tcl.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_2/gt_tcl.htm) for further information.

## Revision History

Revision 2.0	<del>2006 March 01</del>	<del>2.0 public release.</del>
Revision 1.1	<del>2006 January 25</del>	<del>Added release 12.2T to software table.</del>
Revision 1.0	<del>2006 January 25</del>	<del>Initial public release.</del>

## 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>.

---

[Contacts & Feedback](#) | [Help](#) | [Site Map](#) © 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Mar 01, 2006

Document ID: 68840

---