

Table of Contents

<u>Cisco Security Advisory: Cisco Security Advisory: Cisco Catalyst Enable Password Bypass Vulnerability</u>	1
<u>Document ID: 42340</u>	1
<u>Revision 1.4</u>	1
<u>Last Updated 2005 January 05 23:15 (GMT)</u>	1
<u>For Public Release 2003 April 24 08:00 (GMT)</u>	1
<u>Please provide your feedback on this document</u>	1
<u>Summary</u>	1
<u>Affected Products</u>	1
<u>Details</u>	2
<u>Impact</u>	2
<u>Software Versions and Fixes</u>	2
<u>Obtaining Fixed Software</u>	2
<u>Workarounds</u>	3
<u>Exploitation and Public Announcements</u>	3
<u>Status of This Notice: Final</u>	3
<u>Distribution</u>	3
<u>Revision History</u>	4
<u>Cisco Security Procedures</u>	4

Cisco Security Advisory: Cisco Security Advisory: Cisco Catalyst Enable Password Bypass Vulnerability

Document ID: 42340

Revision 1.4

Last Updated 2005 January 05 23:15 (GMT)

For Public Release 2003 April 24 08:00 (GMT)

Please provide your feedback on this document.

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

Summary

Cisco Catalyst software permits unauthorized access to the enable mode in the 7.5(1) release. Once initial access is granted, access can be obtained for the higher level "enable" mode without a password. This problem is resolved in version 7.6(1). Customers with vulnerable releases are urged to upgrade as soon as possible.

This issue is documented in Cisco Bug ID CSCea42030.

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20030424-catos.shtml>.

Affected Products

All users of Cisco Catalyst 4000, 6000, and 6500 with the Catalyst OS software version 7.5(1) only.

No other releases of Cisco Catalyst OS software are affected by this vulnerability. Additionally, Catalyst hardware running Cisco IOS[®] software is not affected by this vulnerability.

No other Cisco products are affected by this vulnerability.

Details

Anyone who can obtain command line access to an affected switch can bypass password authentication to obtain "enable" mode access without knowledge of the "enable" password. If local user authentication is enabled, any username can be used to gain access to the switch without a valid password. This same local user could then enter enable without a valid password.

Command line access is provided through the console, telnet access, or ssh access methods; http access mode is not affected.

This problem was introduced with the local user authentication feature in software version 7.5(1), and is corrected in version 7.6(1).

Bug ID

- CSCea42030

Impact

This vulnerability permits unauthorized access to the configuration mode and unauthorized configuration changes on a Catalyst switch.

Software Versions and Fixes

This vulnerability is repaired in version 7.6(1) which is currently available.

Obtaining Fixed Software

Cisco is offering free software upgrades to remedy this vulnerability for all affected customers. Customers may only install and expect support for the feature sets they have purchased.

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 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 assistance with the upgrade, which should be free of charge.

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

See <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.

Please 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.

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

Workarounds

Use of AAA authentication configurations will eliminate this vulnerability unless configured for fallback to local authentication. AAA configuration information and examples are provided in Configuring TACACS+, RADIUS, and Kerberos on Cisco Catalyst Switches, available at:
http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a0080094ea4.shtml.

Strictly limiting telnet and/or ssh access to the device will prevent the initial connection required to exploit this vulnerability. Telnet and/or ssh access can be controlled with the following command set:

```
set ip permit <address> <mask> telnet
set ip permit <address> <mask> ssh

set ip permit enable
```

This command set will deny all traffic not specified in the permit statements for each protocol.

Additionally, out-of-band management solutions and isolated management VLAN configurations can help mitigate this vulnerability by limiting the initial access necessary for exploitation.

Exploitation and Public Announcements

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

This issue was reported to Cisco by Marco P. Rodrigues.

Status of This Notice: Final

This is a final notice. Although Cisco cannot guarantee the accuracy of all statements in this notice, all the facts have been checked to the best of our ability. Cisco does not anticipate issuing updated versions of this notice unless there is some material change in the facts. Should there be a significant change in the facts, Cisco may update this notice.

Distribution

This advisory will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20030424-catos.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:

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
- bugtraq@securityfocus.com
- full–disclosure@lists.netsys.com
- first–teams@first.org (includes CERT/CC)
- cisco@spot.colorado.edu
- cisco–nsp@puck.nether.net
- comp.dcom.sys.cisco
- Various internal Cisco mailing lists

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.

Revision History

Revision 1.0	24–April–2003	Initial public release.
Revision 1.1	24–April–2003	Added clarification under "Exploitation and Public Announcements" section.
Revision 1.2	25–April–2003	Added customer name that reported issue, corrected details regarding exploitation, and updated workaround information on AAA services.
Revision 1.3	07–May–2003	Added link to AAA configuration examples.
Revision 1.4	05–January–2005	Updated the Configuring TACACS+, RADIUS, and Kerberos on Cisco Catalyst Switches document URL in the Workarounds 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. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

All contents are Copyright © 1992–2005 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Jan 05, 2005

Document ID: 42340
