

[NEWS] Cisco Catalyst Enable Password Bypass Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-04/0054.html>

support_at_securiteam.com

Date: 04/26/03

To: list@securiteam.com

Date: 26 Apr 2003 21:33:57 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

In the US?

Contact Beyond Security at our new California office housewarming rates on automated network vulnerability scanning. We also welcome ISPs and other resellers!

Please contact us at: 323-882-8286 or ussales@beyondsecurity.com

Cisco Catalyst Enable Password Bypass Vulnerability

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.

DETAILS

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

Securiteam: [NEWS] Cisco Catalyst Enable Password Bypass 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).

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) that 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)
- * email: tac@cisco.com.

See <<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>> <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.

Securiteam: [NEWS] Cisco Catalyst Enable Password Bypass Vulnerability

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.

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 that is 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.

ADDITIONAL INFORMATION

The information has been provided by <mailto:psirt@cisco.com> Cisco Systems Product Security Incident Response Team.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.