

Cisco Security Advisory: TACACS+ Authentication Bypass in Cisco Anomaly Detection and Mitigation Products

Document ID: 69073

Advisory ID: cisco-SA-20060215-guard

<http://www.cisco.com/warp/public/707/cisco-sa-20060215-guard.shtml>

Revision 1.0

For Public Release 2006 February 15 1600 UTC (GMT)

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

[Summary](#)

[Affected Products](#)

[Details](#)

[Impact](#)

[Software Versions and Fixes](#)

[Workarounds](#)

[Obtaining Fixed Software](#)

[Exploitation and Public Announcements](#)

[Status of This Notice: FINAL](#)

[Distribution](#)

[Revision History](#)

[Cisco Security Procedures](#)

Summary

A vulnerability in versions 5.0(1) and 5.0(3) of the software used in Cisco Anomaly Detection and Mitigation appliances and service modules may allow unauthorized users to get unauthorized access to the devices and/or escalate their privileges if Terminal Access Controller Access Control System Plus (TACACS+) is incompletely configured.

TACACS+ authentication is disabled by default, and a device correctly configured for TACACS+ authentication is not affected by this vulnerability.

Cisco has made free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20060215-guard.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

This vulnerability affects versions 5.0(1) and 5.0(3) of the software for the Cisco Guard and Cisco Traffic Anomaly Detector appliances *and* the Anomaly Guard Module and Traffic Anomaly Detector Module for the Cisco Catalyst 6500 switches/Cisco 7600 routers if the devices are incompletely configured to use TACACS+ authentication. Please note that 5.0(2) was never released to cisco.com, which is the reason it is not listed as an affected release.

Devices running an affected software version and configured for TACACS+ authentication are vulnerable if the Authentication, Authorization, and Accounting (AAA) command specifies TACACS+ authentication but the configuration lacks the **tacacs-server host** command that specifies the TACACS+ server. In other words, if the configuration includes either or both of the following commands:

```
aaa authentication login tacacs+ local
aaa authentication enable tacacs+ local
```

but *not* the following command:

```
tacacs-server host <IP address of TACACS+ server>
```

the device is vulnerable.

Note: The "local" authentication method specified after the "tacacs+" authentication method in the **aaa authentication** commands above is unrelated to the vulnerability. This authentication method is shown because it is normally used as a fallback in case the TACACS+ server is not available. Devices maybe vulnerable, with or without a "local" authentication method, if the "tacacs+" authentication method is used before the "local" method (if specified) and the configuration lacks the **tacacs-server host** command.

Products Confirmed Not Vulnerable

The Cisco Guard and Cisco Traffic Anomaly Detector are not affected by this vulnerability if they are running the following software versions:

- Versions of the Cisco Guard and Cisco Traffic Anomaly Detector software prior to 5.0. This includes any 3.x and 4.x release.
- Cisco Guard and Cisco Traffic Anomaly Detector software version 5.1 and above.

A Cisco Guard or Cisco Traffic Anomaly Detector running version 5.0(1) or 5.0(3) is not affected if the device is not configured to authenticate users against a TACACS+ server, or if its TACACS+ configuration is complete, i.e. if the **tacacs-server host** command is present in the configuration.

Note: TACACS+ authentication is disabled by default. If no explicit AAA configuration takes place the Cisco Guard and the Cisco Traffic Anomaly Detector will authenticate users against the local database (the "local" authentication method.)

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

Details

The Cisco Guard and Cisco Traffic Anomaly Detector appliances and the Anomaly Guard Module and Traffic Anomaly Detector Module for the Cisco Catalyst 6500 switches/Cisco 7600 routers are Distributed Denial of Service (DDoS) attack mitigation devices that detect the presence of a potential DDoS attack and divert attack traffic destined for the network being monitored without affecting the flow of legitimate traffic.

The Cisco Guard and the Cisco Anomaly Traffic Detector appliances can be managed via a virtual terminal (standard keyboard and monitor attached directly to the appliance), a local serial console, remote Secure Shell (SSH) connections, and/or remote secure web sessions (HTTPS). The Anomaly Guard Module and Traffic Anomaly Detector Module for the Cisco Catalyst 6500 switches/Cisco 7600 routers can be managed by logging into the module from the switch (using the **session** command) as well as remotely via SSH and/or secure web sessions.

TACACS+ is an authentication protocol that provides a way to centrally validate users attempting to gain access to servers, workstations, routers, switches, access servers, and other network devices.

Users accessing the Cisco Guard and the Cisco Anomaly Traffic Detector devices can be authenticated against a local user database that is stored in the device's configuration, or against an external TACACS+ server. A complete configuration to authenticate users against an external TACACS+ server contains the following commands:

```
aaa authentication login tacacs+ local
aaa authentication enable tacacs+ local

tacacs-server host <IP address of TACACS+ server>
```

The **aaa authentication login tacacs+** command configures TACACS+ authentication for users logging into the device via SSH or via the web interface. The **aaa authentication enable tacacs+** command configures TACACS+ authentication for the **enable** command. The **tacacs-server host** command specifies the TACACS+ server.

If the Cisco Guard and the Cisco Anomaly Traffic Detector devices are configured to use an external TACACS+ server to authenticate users logging into the device, but the actual TACACS+ server is not specified with **tacacs-server host** command, then authentication will be bypassed. Privileges that will be granted to the user that bypasses authentication depend on type of account used to log in, and whether the account exists on the device, as follows:

- Non-existent account used: user can only execute **show** commands.
- Existent local account used: user gets the same privileges that are normally granted to that account.
- Existent Linux account used: user gets access to the underlying Linux shell.

In addition, a user can bypass authentication of the **enable** command if enable authentication is performed against a TACACS+ server (via the command **aaa authentication enable tacacs+**) and the actual TACACS+ server is not specified (via the **tacacs-server host** command.)

It is important to note that a device is vulnerable *only* if the **tacacs-server host** command is missing. If this command is present the device is *not* vulnerable, even if the IP address of the server is not correct, and even if the TACACS+ server happens to be unreachable.

This vulnerability is documented in Cisco bug ID [CSCsd21455](#) ([registered](#) customers only) .

Impact

Successful exploitation of the vulnerability presented in this document results in an authentication bypass, and may allow users to elevate the privileges they have been given, allowing full control of the device.

Privilege elevation can potentially be used to sniff traffic, launch Denial-of-Service (DoS) attacks, and to perform network reconnaissance by inspection of the configuration policies.

Software Versions and Fixes

This vulnerability has been resolved in the 5.1 series of the Cisco Guard and Cisco Traffic Anomaly Detector software. The first release in the 5.1 series is 5.1(4).

Software for the Cisco Guard appliance is available for download at <http://www.cisco.com/cgi-bin/tablebuild.pl/cisco-ga-crypto>.

Software for the Cisco Traffic Anomaly Detector appliance is available for download at <http://www.cisco.com/cgi-bin/tablebuild.pl/cisco-ad-crypto>.

Software for the Cisco Anomaly Guard Module for the Cisco Catalyst 6500 switches/Cisco 7600 routers is available for download at <http://www.cisco.com/cgi-bin/tablebuild.pl/cisco-agm-crypto>.

Software for the Cisco Anomaly Traffic Detector Module for the Cisco Catalyst 6500 switches/Cisco 7600 routers is available for download at <http://www.cisco.com/cgi-bin/tablebuild.pl/cisco-adm-crypto>.

When considering software upgrades, also consult <http://www.cisco.com/go/psirt> and any subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, contact the Cisco Technical Assistance Center ("TAC") or your contracted maintenance provider for assistance.

Workarounds

This vulnerability can be completely mitigated if the configuration of TACACS+ authentication is completed by specifying the TACACS+ server via the command **tacacs-server host <IP address of TACACS+ server>**.

As a security best practice, it is recommended that customers make use of the access control feature that restricts connectivity to the SSH and web-based management services to certain IP networks configured by the administrator. This can be accomplished through the **permit wbm** and **permit ssh** commands, which are documented in the following section of the Configuration Guide:

http://cisco.com/en/US/products/ps5888/products_configuration_guide_chapter09186a00804c0a6b.html#wp1162442

Having these access control mechanisms in place may help mitigate the vulnerability in the sense that only users coming from trusted networks will be able to log in.

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 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.

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

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

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.

Exploitation and Public Announcements

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

Cisco would like to thank Gerrit Wenig from Verizon Business for bringing this issue to our attention.

Status of This Notice: FINAL

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.

A stand-alone copy or Paraphrase of the text of this document that omits the distribution URL in the following section is an uncontrolled copy, and may lack important information or contain factual errors.

Distribution

This advisory is posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20060215-guard.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.

- cust-security-announce@cisco.com
- first-teams@first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- comp.dcom.sys.cisco@newsgate.cisco.com

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	2006 February 15	Initial 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>.

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

Updated: Feb 15, 2006

Document ID: 69073
