

[NEWS] TACACS+ Authentication Bypass in Cisco Anomaly Detection and Mitigation Products

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-02/msg00069.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 20 Feb 2006 19:19:25 +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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

TACACS+ Authentication Bypass in Cisco Anomaly Detection and Mitigation Products

SUMMARY

<http://www.rfc-editor.org/cgi-bin/rfcdoctype.pl?loc=RFC&letsgo=1492&type=ftp&file_format=txt> An Access Control Protocol is a new implementation of TACACS made by CISCO..

"

<http://www.cisco.com/en/US/products/ps5888/prod_bulletin0900aecd800fd124.html> Cisco traffic anomaly detection and mitigation solutions deliver the industry's most complete and powerful family of solutions for detecting and defeating complex, sophisticated DDoS attacks."

A vulnerability in Cisco Anomaly Detection and Mitigation appliances and service modules allows unauthorized users to gain access to the devices and/or escalate their privileges if Terminal Access Controller Access Control System Plus (TACACS+) is inadequately configured.

DETAILS

Vulnerable Systems:

- * Cisco Anomaly Detection and Mitigation version 5.0(1)
- * Cisco Anomaly Detection and Mitigation version 5.0(3)

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.

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.

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
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.

Vendor Status:

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

[NEWS] TACACS+ Authentication Bypass in Cisco Anomaly Detection and Mitigation Products

forth at Cisco.com Downloads at
<<http://www.cisco.com/public/sw-center/sw-usingswc.shtml>>
<http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact either "psirt at cisco.com" or "security-alert at cisco.com" for software upgrades.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:psirt@xxxxxxxx>> Cisco Systems Security .

The original article can be found at:
<<http://www.cisco.com/warp/public/707/cisco-sa-20060215-guard.shtml>>
<http://www.cisco.com/warp/public/707/cisco-sa-20060215-guard.shtml>

=====

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@xxxxxxxxxxxxxxxxx
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====
=====

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.