

[Full-Disclosure] Cisco Security Advisory: Default Administrative Password in Cisco Guard and Traffic Anomaly Detector

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-12/0434.html>

From: Cisco Systems Product Security Incident Response Team (*psirt_at_cisco.com*)

Date: 12/15/04

To: full-disclosure@lists.netsys.com

Date: Wed, 15 Dec 2004 15:01:00 -0500

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Cisco Security Advisory: Default Administrative Password in Cisco Guard and Traffic Anomaly Detector

Revision 1.0

For Public Release 2004 December 15 1900 UTC (GMT)

Contents

=====

- 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

=====

The Cisco Guard and Cisco Traffic Anomaly Detector software contains a default password for an administrative account. This password is set, without any user's intervention, during installation of the software used by the Cisco Guard and Traffic Anomaly Detector Distributed Denial of Service (DDoS) mitigation appliances, and is the same in all installations of the product.

Software version 3.0 and earlier of the Cisco Guard and Traffic Anomaly Detector are affected by this vulnerability. Customers running version 3.1 or higher of the software are not affected. There are workarounds available including one that does not require a reboot of the device. Cisco has made free software available to address this problem.

The vulnerabilities are documented as the following Cisco bug IDs: CSCeg12167 and CSCeg12188.

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20041215-guard.shtml>.

Affected Products

=====

Vulnerable Products

All versions of the software for the Cisco Guard and Cisco Traffic Anomaly Detector prior to version 3.1 are affected by this vulnerability.

There are three ways to determine the software version that your Cisco Guard and Cisco Traffic Anomaly Detector DDoS mitigation appliances are running:

- * Virtual terminal or local serial console connection
- * Remote Secure Shell (SSH) connection
- * Remote secure web session

What follows is an example of each method; you should choose the method that applies to your particular environment and network setup.

1. To determine the software version number through the local serial console use a serial cable and a terminal emulation program to connect to the appliance. Once you are connected press the Enter key of your terminal and the Guard and Traffic Anomaly Detector will present, without even logging in, the version of the software running on the devices:

Cisco Guard Version 3.1(0.12)

GUARD login:

In this example the Cisco Guard is running software version 3.1. For a virtual terminal the procedure is the same except that no serial cable or terminal emulation program is needed (a standard keyboard and monitor are directly connected to the appliance.)

2. To obtain the software version number through a SSH session use a SSH client to log into the Cisco Guard or Cisco Traffic Anomaly Detector and issue the show version command–line interface (CLI) command. The following example shows an interaction with a Cisco Traffic Anomaly Detector:

```
prompt$ ssh admin@detector.example.com
admin@detector.example.com's password:
Last login: Wed Nov 24 22:45:53 on ttyS0
admin@DETECTOR#show version
Copyright (c) 2000–2004 Cisco Systems, Inc. All rights reserved.
```

Software License Agreement

[...]

Cisco Anomaly Detector
Release: 3.1(0.12)
Date: 2004/10/27 19:58:14

DETECTOR uptime is 3 weeks, 3 days, 17 hours, 53 minutes
System Serial Number: XXXXXXXX

Contact Information:
Cisco Systems Inc.
riverhead–support@cisco.com
admin@DETECTOR#

In this example the Cisco Traffic Anomaly Detector is running software version 3.1.

3. To obtain the software version that Cisco Guard and Cisco Traffic Anomaly Detector are running through a secure web interface, open the URL [#### Products Confirmed Not Vulnerable](https:// address of your Guard or Detector>/ in a web browser, log in, and then click on the About link located on the top right section of the browser window.</u></div><div data-bbox=)

No other Cisco products are currently known to create these specific default account/passwords.

Details

=====

The Cisco Guard and Cisco Traffic Anomaly Detectors are Distributed Denial of Service (DDoS) attack mitigation appliances 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.

Both 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 SSH connections, and/or remote secure web sessions. Most management and troubleshooting tasks are performed through a CLI interface that is similar to that of most Cisco products, but a special administrative account is provided so certain management and troubleshooting tasks that are not covered by the standard CLI can be performed. The administrative account username is root, like the superuser in the Unix operating system.

This account has a default password that is the same in all installations of the Cisco Guard and Cisco Traffic Anomaly Detector in all versions prior to 3.1. This default password is made up of a combination of letters, numbers, and punctuation per best security practices for passwords, but Cisco recommends that this password be changed for extra security.

The vulnerability described here is documented in the Cisco Bug ID CSCeg12167 for the Cisco Guard and in the Cisco Bug ID CSCeg12188 for the Cisco Traffic Anomaly Detector.

Impact =====

Someone that is able to log into a Cisco Guard or Cisco Traffic Anomaly Detector DDoS mitigation appliance using the root administrative account has full control of the device, which includes the ability to change configurations, divert traffic, and install software.

Software Versions and Fixes =====

While workarounds that do not require a software upgrade exist, Cisco has made available free software that addresses the vulnerability described in this document.

Version 3.1 or later of the Cisco Guard and Cisco Traffic Anomaly Detector software does not leave a default password for the administrative root account after a fresh installation or after an upgrade from previous versions. This is because in version 3.1 and later the installation/upgrade procedure requires the user to choose a password for the administrative account.

Note: the procedure to upgrade to version 3.1 can only be done through the out-of-band interfaces.

When considering software upgrades, please also consult http://www.cisco.com/en/US/products/products_security_advisories_listing.html 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") for assistance.

If affected customers are not able to upgrade the software, the workarounds presented in the Workarounds section can be employed to completely eliminate this vulnerability.

Obtaining Fixed Software

=====

As the fix for this vulnerability is a default configuration change, and a workaround is available, a software upgrade is not required to address this vulnerability. However, if you have a service contract, and wish to upgrade to unaffected code, you may obtain upgraded software through your regular update channels once that software is available. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's Worldwide Web site at <http://www.cisco.com>.

If you need assistance with the implementation of the workarounds, or have questions on the workarounds, please contact the Cisco Technical Assistance Center (TAC).

- * +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.

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>.

Workarounds

=====

The vulnerability described in this document can be eliminated completely by logging into the affected Cisco Guard and Cisco Traffic Anomaly Detector DDoS mitigation appliances and changing the default password for the administrative root account to a strong password chosen by the user.

To change the default password you need to run the `passwd` command once you have logged in as the root user. The following interaction shows an example of a change password dialog in a Cisco Traffic Anomaly Detector that is performed via SSH:

```
prompt$ ssh root@detector.example.com
root@detector.example.com's password:
Last login: Tue Nov 23 15:48:13 on ttyS0
[root@DETECTOR root]# passwd
Changing password for user root.
New password: <new password typed in here>
Retype new password: <new password typed in here>
passwd: all authentication tokens updated successfully.
```

In order to perform this procedure you will need the default password. To obtain this password customers must contact the Cisco TAC. Entitlement will be checked so please have your product serial number available and give the URL of this notice.

After changing the default password, the Cisco Guard and Traffic Anomaly Detector will not accept root logins using the default password.

A reboot is not required for the new password to take effect, so network operations will not be disrupted.

If affected customers do not wish to contact Cisco to obtain the default password, it is possible to change the administrative account's password by performing the password recovery procedure. This procedure is documented at the following location:

http://cisco.com/en/US/products/ps5887/products_password_recovery09186a008037942b.shtml

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. Refer to the documentation for your Cisco Guard and Cisco Traffic Anomaly Detector, specifically the `permit wbm` and `permit ssh` commands, for details on how to enable this feature. Having these access control mechanisms in place may mitigate the vulnerability if it cannot be eliminated completely by changing the default password as described above.

Exploitation and Public Announcements

=====

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

This vulnerability was uncovered during internal code audit.

Status of This Notice: FINAL

=====

THIS ADVISORY IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY. YOUR USE OF THE INFORMATION ON THE ADVISORY OR MATERIALS LINKED FROM THE ADVISORY IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS NOTICE AT ANY TIME.

Distribution

=====

This advisory will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20041215-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 (includes CERT/CC)
- * bugtraq@securityfocus.com
- * vulnwatch@vulnwatch.org
- * cisco@spot.colorado.edu
- * cisco-nsp@puck.nether.net
- * full-disclosure@lists.netsys.com
- * 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	Initial
1.0	2004-December-15 public release.

Cisco Security Procedures

=====

Full-Disclosure: [Full-Disclosure] Cisco Security Advisory: Default Administrative Password in Cisco Guard and Traffic Anoma

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>.

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.2.5 (GNU/Linux)

iD8DBQFBwJadezGozzK2tZARAvqjAJ0VQ8rC3EpQQZVeICjfQbB5/WY3EgCg985B
KdQz4NFAbwgoDaInXmWjs7c=
=chLH

-----END PGP SIGNATURE-----

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>

[Full-Disclosure] Cisco Security Advisory: Default Administrative Password in Cisco Guard and Traffic Anoma