

# Table of Contents

<b><u>Cisco Security Notice: Response to BugTraq – Cisco 6509 Switch Telnet Vulnerability</u></b> .....	1
<u>Revision 1.0</u> .....	1
<u>Last Updated 2003 October 4</u> .....	1
<u>Please provide your feedback on this document</u> .....	1
<u>Summary</u> .....	1
<u>Details</u> .....	1
<u>Cisco Security Procedures</u> .....	2

# Cisco Security Notice: Response to BugTraq – Cisco 6509 Switch Telnet Vulnerability

## Revision 1.0

Last Updated 2003 October 4

---

Please provide your feedback on this document.

---

**Summary**  
**Details**  
**Cisco Security Procedures**

---

## Summary

This document is provided to simplify access to Cisco responses to possible product security vulnerability issues posted in public forums for Cisco customers. This does not imply that Cisco perceives each of these issues as an actual product security vulnerability. This notice is provided on an "as is" basis and does not imply any kind of guarantee or warranty. Your use of the information on the page or materials linked from this page are at your own risk. Cisco reserves the right to change or update this page without notice at any time.

## Details

Original Report: <http://www.securityfocus.com/archive/1/340193> . Cisco responded with the following, which is also archived at <http://www.securityfocus.com/archive/1/340241> .

```
To: BugTraq
Subject: Re: Cisco 6509 switch telnet vulnerability
Date: Oct 4 2003 1:11AM Author: Wendy Garvin <wgarvin@cisco.com>
Message-ID: <20031004011131.GA1361@cisco.com>
In-Reply-To: <20031003000326.4614.qmail@sf-www2-symnsj.securityfocus.com>
```

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1
```

Chris,

This is a known bug, and we were able to reproduce the behavior you reported, however the commands cannot actually be executed. As you demonstrated, you can get the 'help' text for non-enable commands at the password prompt, but the command is not completed, all that is returned is an error message. These commands are publicly available:

[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw\\_5\\_5/cmd\\_refr/cli.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_5_5/cmd_refr/cli.htm)

This bug cannot be used to gain control of the switch, gather further information about the device or gather details about the traffic it carries. It is documented as CSCdr87435, and it is fixed in 5.5(3) and later, and 6.1(1) and later. Details about the problem can be found on our website if you are a registered user:

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCdr87435>

Thank you for your work on this problem. As always, working with the Cisco PSIRT team is the best way to verify the accuracy of information before posting it publicly.

- ---Wendy

> Chris Norton <kicktd hotmail com> [2003-10-03 16:24] wrote:

>

>

> A vulnerability has been found on Cisco 6509 switches. The vulnerability was found to work on 2 different Cisco 6509 switches running CATOS 5.4(2) and 5.5(2). The vulnerability can lead to information and commands being executed on the remote switch from the login prompt. Commands can be executed at the Enter password: prompt as long as they are followed by a space and a ?

> Proof of concept below:

> Cisco Systems Console

>

> Enter password:

> <data\_size> Size of the packet (0..1420)

> <cr>

> Enter password: traceroute 127.0.0.1

>

> This vulnerability has yet to be confirmed by Cisco but they have been alerted about it.

>

> [ ----- End of Included Message ----- ]

- ---

Wendy Garvin - Cisco PSIRT - 408 525-1888 CCIE# 6526

-----

<http://www.cisco.com/go/psirt>

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

Version: PGP 6.5.2

iQA/AwUBP34brc/6vhuARK9tEQICAgCgj7ghQcOp0po07TPsRyHEI+oe50MAoOBo

BHjtXy3ob12Ss7bouy3JpARY

=RIWI

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

## 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/warp/public/707/sec\\_incident\\_response.shtml](http://www.cisco.com/warp/public/707/sec_incident_response.shtml). 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 © 1992–2004 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.