

Table of Contents

<u>Cisco Security Notice: Response to BugTraq – show Command Vulnerability</u>	1
<u>Revision 1.0</u>	1
<u>For Public Release 2000 May 09</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>	3

Cisco Security Notice: Response to BugTraq – show Command Vulnerability

Revision 1.0

For Public Release 2000 May 09

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/1/58169> . Cisco responded with the following, which is also archived at <http://www.securityfocus.com/archive/1/59434> .

```
To: BugTraq
Subject: Re: Possible issue with Cisco on-line help?
Date: May 9 2000 2:30PM
Author: Lisa Napier <lnapier@cisco.com>
Message-ID: <4.2.0.58.20000508173724.08f34e70@twoguys>
In-Reply-To: <20000504120430.17546.qmail@securityfocus.com>
```

Hi Fernando,

I confirmed this behavior, and found some history on why we did things this way.

The original intent of showing a limited subset of commands at the "show ?" help command was to simplify the command line help subsystem. When user typed the command "show ?", we intended to provide them a list of only the most used and useful commands at that level.

To allow customers to see all the commands available at that level, the command "terminal full-help" was implemented in October of 1993.

The intent was not security related at all, but simply an attempt to provide only the 'useful' commands to the users who were supposed to be at that prompt and at that level, rather than having them scroll through several screens of available but not very useful commands.

So, rather than being an inadvertent mistake in the parser, this is actually how the

product was designed.

I will be updating our white papers on securing routers to include the recommendation of setting the default user privilege level to 0, and ensuring that only commands that are explicitly permitted to be run by un-enabled users are set to priv level 0.

Thanks much for your work on this Fernando,

Lisa Napier
Product Security Incident Response Team
Cisco Systems
http://www.cisco.com/warp/public/707/sec_incident_response.shtml

At 12:04 PM 05/04/2000 +0000, Fernando Montenegro wrote:

```
>Hi!
>
>I have received information from Matti Saarinen
><mjs cc tut fi> explaining how the on-line help can be
>configured to show all the commands available (see below).
>
>This explains the apparent lack of authorization control
>over the "show" options.
>
>It seems that the only issue left is that there is so much
>information available from the non-enabled account.I would
>think that, on account of that, the recommendation for
>"jailing" the user still applies, though.
>
>Cheers,
>Fernando
>
>
>Extracts from the message received from Matti Saarinen
><mjs cc tut fi> :
>
> > Router2>show ?>      backup          Backup status
> >   cef                Cisco Express Forwarding
> >   clock              Display the system clock
> >   dialer             Dialer parameters and statistics
> >   flash:             display information about flash: file>
>system
> >   history            Display the session command history>
>...>
> > Notice that we did not see an "access-lists" option, so
>the
> > help system thinks we should not be able to run it...
>       Yes, you cannot normally see access-lists option in
>       the output of the help system.
>router>sh ?
>  alps                Alps information
>  atm                 ATM information
>  backup              Backup status[cut]
>
>       But when you enable full help the access-lists
>option is there
>       with many others:
>router>terminal full-help
>router>sh ?
>  access-expression  List access expression
>  access-lists       List access lists
>  adjacency          Adjacent nodes
>  aliases            Display alias commands
>  alps               Alps information
```

```
> arp                ARP table
> async             Information on terminal lines used as
>router interfaces
> atm              ATM information
> backup           Backup status
>                 And the privilege level was 1 the whole time:
>router>sh priv
>Current privilege level is 1
```

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. 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.