

# Table of Contents

<b><u>Cisco Security Notice: Response to BugTraq – Catalyst 3500 Issue</u></b> .....	<b>1</b>
<u>Revision 1.0</u> .....	1
<u>Last Updated 2000 November 13</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 – Catalyst 3500 Issue

## Revision 1.0

Last Updated 2000 November 13

---

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/1/141471> . Cisco responded with the following, which is also archived at <http://www.securityfocus.com/archive/1/144655> .

```
To: BugTraq
Subject: Re: 3500XL
Date: Nov 13 2000 7:35PM
Author: Damir Rajnovic <gaus cisco com>
Message-ID: <4.2.0.58.20001113202752.06ad4d90@amsterdam.cisco.com>
```

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

Hello there,

This is the official reply to the def-2000-02, Defcom Labs Advisory, posted on 2000-October-26 by Olle Sergerdahl (see <http://www.securityfocus.com/bid/1846>)

This is the brief description from the def-2000-02 advisory:

"The Catalyst 3500 XL series switches web configuration interface lets any user execute any command on the system without logging in.

This issue was extremely easy to find, as Cisco provides a link to it from the first page of the web configuration service. This is one of the reasons I have decided to go public with the issue so soon."

We investigated this issue and found that this holds only if user did not configured an enable password. The only instance when

this is true is when switch administrator has configured an access password (on vty lines) but without an enable password. This situation may be confusing since admins will be prompted for a password when trying to telnet to the switch but will not be asked for it when using the Web to access the switch. All switches from 2900XL and 3500XL families share this behavior.

We suspect that this scenario was present when Olle made his discovery, but have not yet received his configuration to confirm.

Cheers,

Gaus

-----BEGIN PGP SIGNATURE-----  
Version: PGPfreeware 6.0.2i

iQCVAwUBOhBQZMAFeg0PniW5AQHUDAQAoU7Th2I1DhmZXXq952HTli9VWFURHGJV  
8Zq4e19agp+0BrlpHgilo5zjlfk0LikEuTqCTpNrYCD8Ng8oI/eNGYfsV4oOYNh5  
LY/YyuVWt0bnEGkSlRryazWfMpHs5Vbg5nLbyXEr3XgYzycTIs+s/ItmlAOs7BE9  
wbu38N30lwA=  
=HRnz  
-----END PGP SIGNATURE-----

=====  
Damir Rajnovic <psirt cisco com>, PSIRT Incident Manager, Cisco Systems  
<[http://www.cisco.com/warp/public/707/sec\\_incident\\_response.shtml](http://www.cisco.com/warp/public/707/sec_incident_response.shtml)>  
Phone: +44 7715 546 033  
4 The Square, Stockley Park, Uxbridge, MIDDLESEX UB11 1BN, GB  
=====  
There is no insolvable problems. Question remains: can you  
accept the solution?

## 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.