

Table of Contents

<u>Cisco Security Notice: Response to BugTraq – Cisco AS5350 Crashes with nmap Connect Scan</u>	1
<u>Revision 1.0</u>	1
<u>Last Updated 2002 October 29</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 AS5350 Crashes with nmap Connect Scan

Revision 1.0

Last Updated 2002 October 29

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/1/297457> . Cisco responded with the following, which is also archived at <http://www.securityfocus.com/archive/1/297710> .

To: BugTraq
Subject: Re: CISCO as5350 crashes with nmap connect scan
Date: Oct 29 2002 10:31PM
Author: Wendy Garvin <wgarvin@cisco.com>
Message-ID: <20021029223138.GB17617@cisco.com>

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

Thomas,

I appreciate your communication with Cisco PSIRT on September 9th regarding questions on a 5350. Your original problem was due to a misconfiguration, and appropriate configuration details were provided within a day of your request. No crash was mentioned to us.

This evening I have worked in the lab on both a 5300 and a 5350 running 12.2(11)T. I have run nmap as you suggested with a slight change, there is no -d option, I assume you meant -Tinsane. I have been unable to reproduce your results.

Cisco takes vulnerabilities with our devices very seriously, and if you can show us how to reproduce this problem, we'd be very interested in fixing it. Please contact us with detailed version information and any specifics on your setup, and we'd be happy to continue working with you.

As always, the appropriate way to contact us is by emailing psirt cisco com
For technical assistance and configuration issues, please contact
tac cisco com

Thank you,

- -Wendy

- - -

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

- -----
http://www.cisco.com/go/psirt

> Thomas Munn <munn bigfoot com> [2002-10-28 14:52] wrote:
>
>
> I have managed to "reduplicate" at least five times the
> following scenario with a cisco as5250, with firmwreare
> 12.2 (11t) release firmware of cisco:
>
> nmap -dinsane -p 1-65535 ip.of.as5350 This causes a
> "hard" lockup, and the device must be powered off in
> order to have functionality restored to it.
>
> Mentioned to PSIRT at cisco, they didn't do anything.
>
> Sincerely,
>
> Thomas J. Munn
>
> [----- End of Included Message -----]

-----BEGIN PGP SIGNATURE-----
Version: PGP 6.5.2

iQA/AwUBPb32BZPS/wbyNnWcEQLRmwCdFq+tAX9zRxktmZW5DRZ4YNArmXcAoLy/
fygu/v2CA8NihUn/C00v2Hpf
=0REH
-----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. 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.