

Table of Contents

<u>Cisco Security Notice: Response to BugTraq – Cisco IOS Software – Three Possible DoS Attacks</u>	1
<u>Revision 1.0</u>	1
<u>Last Updated 2002 June 06</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 – Cisco IOS Software – Three Possible DoS Attacks

Revision 1.0

Last Updated 2002 June 06

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/1/275587> . Cisco responded with the following, which is also archived at <http://www.securityfocus.com/archive/1/275963> .

```
To: BugTraq
Subject: Re: Three possible DoS attacks against some IOS versions.
Date: Jun 6 2002 10:51PM
Author: Sharad Ahlawat <sahlawat cisco com>
Message-ID: <200206061551.59472.sahlawat@cisco.com>
In-Reply-To: <20020605175215.6341.qmail@mail.securityfocus.com>
```

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

Hash: SHA1

This email is in response to the BugTraq posting at
<http://online.securityfocus.com/archive/1/275587/2002-06-03/2002-06-09/0>

There are three issues in the original email, their responses are given below.

Issue 1.

=====

A Cisco 2621 router with 12.1(6a) could not be crashed by using the nmap command and by mirroring the setup, used by Andrew. Other IOS releases were tried and no crashes were observed. This currently seems to be a setup specific issue.

Andrew was using an Interim release of IOS during his testing. Interim releases are built at regular intervals between maintenance releases

and receive less testing. Interim releases should be selected only if there is no other suitable release that addresses an issue, and interim images should be upgraded to the next available maintenance release as soon as possible. Interim releases are not available via manufacturing, and usually are not available for customer download from CCO without prior arrangement with the Cisco TAC.

I have published 12.1(6a) for Andrew to have him test in his network setup. I will have a followup conversation with him on this.

Issue 2.

=====

UDP port 1985 found open when no HSRP configured. Cisco Bug ID CSCdt64533 - has already been integrated in 12.2.

High CPU utilization is expected behavior when one directs a continuous stream of data at any open port, as the data needs to be processed by the router. Streaming UDP traffic at a Cisco 2621 router's port 1985 does not freeze the router though it has been observed on lower end routers to cause high CPU utilization and unresponsiveness, but no spontaneous reboots.

Issue 3.

=====

an excerpt from RFC 2281 - Cisco HSRP

7. Security Considerations

This protocol does not provide security. The authentication field found within the message is useful for preventing misconfiguration. The protocol is easily subverted by an active intruder on the LAN. This can result in a packet black hole and a denial-of-service attack. It is difficult to subvert the protocol from outside the LAN as most routers will not forward packets addressed to the all-routers multicast address (224.0.0.2).

- ----

Cisco is considering using MD5 to improve the protection of HSRP in future releases of IOS.

However, there are some other factors that must be considered in this context:

- - this vulnerability can be exploited only from the local segment (not over the Internet).
- - the same effect, denial of service, can be produced by using ARP, which can not be protected in any way.

The last factor is especially important since it may cause a false sense of security if the user is using a hardened version of HSRP as an attacker can still disrupt the network by using crafted ARP packets.

Another aspect of this issue is that in its current implementation, HSRP doesn't seem to perform a validity check on the IP addresses. This is under active investigation as Cisco Bug ID CSCdu38323.

Cisco HSRP documentation can be found at -
<http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs009.htm>

- --

Sharad Ahlawat.

Product Security Incident Response Team (PSIRT) Incident Manager

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

Phone:+1 (408) 527-6087 (Land line and Mobile)
DH/DSS key Id: 0xC12A996C
Fingerprint: 9A93 2A20 43E5 7F01 2954 C427 1A81 A898 C12A 996C

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 Web site at <http://www.cisco.com/go/psirt>.

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

Version: GnuPG v1.0.7 (GNU/Linux)

iD8DBQE8/+eLGoGomMEqmWwRAvQuAKDD0QUix/yYu+9R7ZgdJh0AK8pQdACeNa8q
ENh90WxBZqYLg3sjuLjxE0w=
=pCHF
-----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.