

Table of Contents

<u>Cisco Security Notice: Response to BugTraq – HSRP Issues</u>	1
<u>Revision 1.0</u>	1
<u>Last Updated 2001 May 16</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 – HSRP Issues

Revision 1.0

Last Updated 2001 May 16

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/1/182008> . Cisco responded with the following, which is also archived at <http://www.securityfocus.com/archive/1/184814> .

```
To: BugTraq
Subject: Re: Cisco HSRP Weakness/DoS
Date: May 16 2001 7:42AM
Author: Damir Rajnovic <gaus cisco com>
Message-ID: <4.3.2.7.2.20010516074146.023c1d50@144.254.74.238>
```

Hello,

Seems that this mail has been lost again.

Gaus

```
=====
My previous mail seems to be lost due to the mail server problems
so here is the response again.
```

In response to this mail sent by bashis on Bugtraq:

```
At 19:57 03/05/2001 +0200, bashis wrote:
>I was playing with Cisco's HSRP (Hot Standby Routing Protocol),
>and there is a (major) weakness in that protocol that allow
>any host in a LAN segment to make a HSRP DoS.
[truncated, see http://www.securityfocus.com/archive/1/182008]
```

We can confirm that described vulnerability is present in the HSRP

and, at the present time, there is no workaround for it.

Cisco is deliberating usage of IP authenticated header for HSRP and VRRP (Virtual Router Redundancy Protocol, RFC2338) in the 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 issue is especially important since it may cause a false sense of security if user is using a hardened version the protocol (whichever protocol). Even by using VRRP and ESP+AH option, an attacker can still disrupt the network by using ARP.

Regards,

Gaus

=====

Damir Rajnovic <psirt cisco com>, PSIRT Incident Manager, Cisco Systems
<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. 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.