

Cisco Security Notice: Response to BugTraq – Cisco EIGRP Issue

Document ID: 60557

Revision 1.0

Last Updated 2002 December 19

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.phenoelit.de/stuff/CiscoEIGRP.txt>.

Cisco responded with the following, which is also archived at http://www.cisco.com/warp/public/707/eigrp_issue.html:

Cisco can confirm the statement made by FX from Phenoelit in its message "Cisco IOS EIGRP Network DoS" posted on 2002-Dec-19. The EIGRP implementation in all versions of IOS is vulnerable to a denial of service if it receives a flood of neighbor announcements. EIGRP is a Cisco extension of IGP routing protocol used to propagate routing information in internal network environments.

The workaround for this issue is to apply MD5 authentication that will permit the receipt of EIGRP packets only from authorized hosts. You can find an example of how to configure MD5 authentication for EIGRP at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/np1_c/1cp1/1ceigrp.htm#xtocid18

If you are using EIGRP in the unicast mode then you can mitigate this issue by placing appropriate ACL which will block all EIGRP packets from illegitimate hosts. In the following example, the EIGRP neighbor has IP address of 10.0.0.2 and the local router has address 10.0.0.1.

```
Router# config term
Router(config)# access-list 111 permit eigrp host 10.0.0.2 host 10.0.0.1
Router(config)# access-list 111 deny eigrp any host 10.0.0.1
```

The previous example permits all EIGRP packets throughout the router and into the rest of the network. If you want to block these packets as well then use the following commands instead of the previous example:

```
Router# config term  
Router(config)# access-list 111 permit eigrp host 10.0.0.2 host 10.0.0.1  
Router(config)# access-list 111 deny eigrp any any
```

An ACL will not be effective if you are using the default multicast mode of EIGRP neighbor discovery. However, multicast packets should not be propagated through the Internet so an attacker must be on the same local network segment as the target router in order to exploit this issue with multicast advertisements.

At the time of writing this notice Cisco PSIRT does not have a current estimate on when the fix will be available.

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/en/US/products/products_security_vulnerability_policy.html. 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 © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Dec 19, 2002

Document ID: 60557
