

Table of Contents

<u>Cisco Security Notice: Cisco's Response to the EIGRP Issue</u>	1
<u>For Public Release 2002 December 20</u>	1
<u>Please provide your feedback on this document</u>	1
<u>Summary</u>	1
<u>Workarounds</u>	1

Cisco Security Notice: Cisco's Response to the EIGRP Issue

For Public Release 2002 December 20

Please provide your feedback on this document.

Summary
Workarounds

Summary

This is not a Cisco Security Advisory.

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's extension of IGP routing protocol used to propagate routing information in internal network environments.

Workarounds

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.
