

Cisco Security Response: Cisco IOS OSPF Exploit

Document ID: 40762

<http://www.cisco.com/warp/public/707/cisco-sr-20030220-ospf.s>

Revision 1.1

Last Updated 2004 July 19 0800 GMT UTC (GMT)

For Public Release 2003 February 20 0800 GMT UTC (GMT)

Please provide your feedback on this document.

Cisco Response
Additional Information
Revision History
Cisco Security Procedures

Cisco Response

This is not a Cisco Security Advisory.

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.

Additional Information

The original report is located at <http://www.securityfocus.com/archive/1/312510> . Cisco responded with the following, which is also archived at <http://www.securityfocus.com/archive/1/312802> .

Cisco can confirm the statement made by FX from Phenoelit in his message "Cisco IOS OSPF exploit" posted on 2003-Feb-20. The Open Shortest Path First (OSPF) implementation in certain Cisco IOS® software versions is vulnerable to a denial of service if it receives a flood of neighbor announcements in which more than 255 hosts try to establish a neighbor relationship per interface.

One workaround for this issue is to configure OSPF MD5 authentication. This may be done per interface or per area. For more information, refer to documentation on configuring MD5 authentication at <http://www.cisco.com/warp/customer/104/25.shtml#4> (registered customers only) .

Another possible workaround is to apply inbound access lists to explicitly allow certain OSPF neighbors only, as demonstrated below.

```
access-list 100 permit ospf host a.b.c.x host 224.0.0.5
```

```
access-list 100 permit ospf host a.b.c.x host interface_ip
access-list 100 permit ospf host a.b.c.y host 224.0.0.5
access-list 100 permit ospf host a.b.c.y host interface_ip
access-list 100 permit ospf host a.b.c.z host 224.0.0.5
access-list 100 permit ospf host a.b.c.z host interface_ip
access-list 100 permit ospf any host 224.0.0.6
access-list 100 deny ospf any any
access-list 100 permit ip any any
```

Cisco IOS software versions 11.1 through 12.0 are subject to this vulnerability. This bug has been resolved. The following versions of Cisco IOS software are the first fixed releases, meaning that any subsequent releases also contain the fix.

- 12.0(19)S
- 12.0(19)ST
- 12.1(1)
- 12.1(1)DB
- 12.1(1)DC
- 12.1(1)T

We would like to thank FX for his continued cooperation with us in the spirit of responsible disclosure and working to increase awareness of security issues.

For information on working with the Cisco PSIRT regarding potential security issues, please see our contact information at http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html#Problems.

This issue was originally reported on the Bugtraq mailing list at <http://www.securityfocus.com/archive/1/312510> , and Cisco responded at <http://www.securityfocus.com/archive/1/312802> , and with this notice.

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

Revision History

Revision 1.1	2004 July 19	Last updated.
Revision 1.0	2003 February 220	Initial public release.

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 © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.
