

Table of Contents

<u>Cisco Security Notice: Exploit for Multiple Cisco Vulnerabilities</u>	1
<u>Revision 1.3</u>	1
<u>Last Updated 2004 May 07 at 17:30 UTC (GMT)</u>	1
<u>For Public Release 2004 March 27 19:30 UTC</u>	1
<u>Please provide your feedback on this document</u>	1
<u>Summary</u>	1
<u>Details</u>	1
<u>Workarounds</u>	3
<u>Status of This Notice: INTERIM</u>	3
<u>Revision History</u>	3
<u>Cisco Security Procedures</u>	3

Cisco Security Notice: Exploit for Multiple Cisco Vulnerabilities

Revision 1.3

Last Updated 2004 May 07 at 17:30 UTC (GMT)

For Public Release 2004 March 27 19:30 UTC

Please provide your feedback on this document.

Summary

Details

Workarounds

Status of This Notice: INTERIM

Revision History

Cisco Security Procedures

Summary

Proof-of-concept code has been publicly released by an external group that exploits multiple previous vulnerabilities in various Cisco products.

Details

Proof-of-concept code has been publicly released by an external group that exploits multiple previous vulnerabilities in various Cisco products. The following list of vulnerabilities taken verbatim from the exploit code are affected. Included after each is a URL which may be referenced for more information regarding each vulnerability where Cisco has previously released a security advisory or response to address the issue. Customers should take steps to ensure that they have addressed each of these either via a software upgrade or workarounds in place as appropriate in order to mitigate any risk from this new exploit code.

1. Cisco 677/678 Telnet Buffer Overflow Vulnerability

CBOS – Improving Resilience to Denial-of-Service Attacks

<http://www.cisco.com/warp/public/707/CBOS-DoS.shtml>

2. Cisco IOS Router Denial of Service Vulnerability

Cisco IOS HTTP Server Vulnerability

<http://www.cisco.com/warp/public/707/ioshttpserver-pub.shtml>

3. Cisco IOS HTTP Auth Vulnerability

IOS HTTP Authorization Vulnerability

<http://www.cisco.com/warp/public/707/IOS-httplevel-pub.html>

4. Cisco IOS HTTP Configuration Arbitrary Administrative Access Vulnerability

IOS HTTP Authorization Vulnerability

<http://www.cisco.com/warp/public/707/IOS-httplevel-pub.html>

5. Cisco Catalyst SSH Protocol Mismatch Denial of Service Vulnerability

Cisco Catalyst SSH Protocol Mismatch Vulnerability

<http://www.cisco.com/warp/public/707/catalyst-ssh-protocolmismatch-pub.shtml>

6. Cisco 675 Web Administration Denial of Service Vulnerability

Multiple Vulnerabilities in CBOS

<http://www.cisco.com/warp/public/707/CBOS-multiple.shtml>

7. Cisco Catalyst 3500 XL Remote Arbitrary Command Vulnerability

Catalyst 3500 Issue

Report: <http://www.securityfocus.com/archive/1/141471>

Cisco Response: <http://www.securityfocus.com/archive/1/144655>

8. Cisco IOS Software HTTP Request Denial of Service Vulnerability

Cisco IOS HTTP Server Query Vulnerability

<http://www.cisco.com/warp/public/707/ioshttpserverquery-pub.shtml>

9. Cisco 514 UDP Flood Denial of Service Vulnerability

A Vulnerability in IOS Firewall Feature Set

<http://www.cisco.com/warp/public/707/IOS-cbac-dynacl-pub.shtml>

10. CiscoSecure ACS for Windows NT Server Denial of Service Vulnerability

Web Interface Vulnerabilities in Cisco Secure ACS for Windows

<http://www.cisco.com/warp/public/707/ACS-Win-Web.shtml>

11. Cisco Catalyst Memory Leak Vulnerability

Cisco Catalyst Memory Leak Vulnerability

<http://www.cisco.com/warp/public/707/catalyst-memleak-pub.shtml>

12. Cisco CatOS CiscoView HTTP Server Buffer Overflow Vulnerability

Cisco CatOS Embedded HTTP Server Buffer Overflow

<http://www.cisco.com/warp/public/707/catos-http-overflow-vuln.shtml>

13. %u Encoding IDS Bypass Vulnerability (UTF)

Cisco Secure Intrusion Detection System Signature Obfuscation Vulnerability

<http://www.cisco.com/warp/public/707/cisco-intrusion-detection-obfuscation-vuln-pub.shtml>

14. Cisco IOS HTTP Denial of Service Vulnerability

Cisco IOS HTTP Server Query Vulnerability

<http://www.cisco.com/warp/public/707/ioshttpserverquery-pub.shtml>

Workarounds

Possible workarounds for each of the vulnerabilities may be found in the advisories referenced in the Details section.

Status of This Notice: INTERIM

This is an interim notice. Although Cisco cannot guarantee the accuracy of all statements in this notice, all of the facts have been checked to the best of our ability. Cisco does not anticipate issuing updated versions of this notice. Should there be a change in the facts, Cisco may update this notice.

A stand-alone copy or paraphrase of the text of this security notice that omits the distribution URL in the following section is an uncontrolled copy, and may lack important information or contain factual errors.

Revision History

Revision 1.3	2004-May-07	Updated notice to include exploits 11-14 in the Details section.
Revision 1.2	2004-April-06	Updated #6 in the Details section.
Revision 1.1	2004-April-02-0000 UTC (GMT)	Updated notice to include exploit #10 in the Details section.
Revision 1.0	2004-March-26	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 © 1992–2004 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.