

Table of Contents

<u>Cisco Security Notice: Vulnerability in a Variant of the TCP Timestamps Option</u>	1
<u>Document ID: 64909</u>	1
<u>Revision 1.1</u>	1
<u>For Public Release 2005 May 18 1600 UTC (GMT)</u>	1
<u>Please provide your feedback on this document</u>	1
<u>Summary</u>	1
<u>Details</u>	1
<u>Symptoms</u>	1
<u>Affected Products</u>	2
<u>Unaffected Products</u>	2
<u>Status of This Notice: FINAL</u>	3
<u>Revision History</u>	3
<u>Cisco Security Procedures</u>	3
<u>Related Information</u>	3

Cisco Security Notice: Vulnerability in a Variant of the TCP Timestamps Option

Document ID: 64909

Revision 1.1

For Public Release 2005 May 18 1600 UTC (GMT)

Please provide your feedback on this document.

Summary
Details
Symptoms
Affected Products
Unaffected Products
Status of This Notice: FINAL
Revision History
Cisco Security Procedures
Related Information

Summary

Some implementations of the Transmission Control Protocol (TCP) Timestamps option (RFC1323) are vulnerable to a Denial of Service (DoS) attack from specifically crafted packets.

Only certain implementations of the TCP Timestamps option are vulnerable.

This notice will be posted at <http://www.cisco.com/warp/public/707/cisco-sn-20050518-tcps.shtml>.

Details

TCP is defined in RFC 793 as a means to provide reliable transmission between hosts in packet-switched computer networks. RFC 1323 introduces the TCP timestamps option to increase the performance of TCP. Some implementations of the TCP timestamps option are vulnerable to a Denial of Service (DoS) attack from specifically crafted packets. The impact of a successful attack is a stall of a TCP connection until the TCP connection is reset. Only the TCP session that is explicitly targeted will be affected. All other active TCP sessions will be unaffected.

An attacker needs to determine the IP addresses and the TCP port numbers of both the source and the destination to exploit this vulnerability. Only the TCP sessions that are originating or terminating on a targeted system can be affected. All TCP sessions passing through a targeted system are unaffected.

Symptoms

A successful exploitation will result in stalling the targeted TCP connection. Other active TCP sessions will stay unaffected. A stalled TCP connection can be cleared by resetting the TCP connection.

Affected Products

The following Cisco products are affected by this vulnerability:

- SN5400 series storage routers
This issue is addressed by CSCin85370 for SN5400 series storage routers.
- CSS11000 series content services switches
This issue is addressed by CSCeh40395 for CSS11000 series
- AP350 and AP1200 series Access Points
Only the access points that are running VxWorks are affected by this vulnerability. Access points that are running Cisco IOS® are not affected. Systems that are running VxWorks can be upgraded to Cisco IOS to address this issue. Refer to the following URL for more information on upgrading access points to Cisco IOS:
http://www.cisco.com/en/US/products/hw/wireless/ps430/products_tech_note09186a008019fea0.shtml
- MGX series WAN switches
This issue is documented by CSCeh85125 for MGX8200 series and CSCeh85130 for MGX8800 and MGX8900 series switches. These systems use TCP only for management services (i.e., telnet and ssh) and are only vulnerable for these services.
- Microsoft Security Bulletin MS05–019 addresses this vulnerability for Microsoft Windows Operating System (OS). The following Cisco products that are running on Microsoft Windows are vulnerable, if they do not include the patch for MS05–019 .
 - ◆ Cisco CallManager
 - ◆ Cisco Conference Connection
 - ◆ Cisco Emergency Responder
 - ◆ Cisco MeetingPlace
 - ◆ Cisco Personal Assistant
 - ◆ Cisco Intelligent Contact Management Product Family
 - ◆ Cisco IP Contact Center Product Family
 - ◆ Cisco Interactive Voice Response Product Family
 - ◆ Cisco Remote Monitoring Suite Option
 - ◆ Cisco Web Collaboration Option
 - ◆ Cisco E–Mail Manager Option
 - ◆ Cisco Agent Desktop
 - ◆ Cisco Support Tools
 - ◆ Cisco Unity
 - ◆ Cisco Secure ACS
 - ◆ CiscoWorks

Unaffected Products

Only the products that are explicitly listed above are affected. All other products **including**, but **not limited** to:

- Cisco IOS
- Cisco IOS–XR
- Cisco CatOS
- Cisco PIX OS

are unaffected. These products are listed for reference only. Any product that is not explicitly mentioned is unaffected.

Status of This Notice: FINAL

This is a final 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 unless there is some material change in the facts. Should there be a significant 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 1.1	2005-May-23	Added two products to Microsoft Security Bulletin list under Affected Products.
Revision 1.0	2005-May-18	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/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>.

Related Information

- **CERT/CC Vulnerability Note**

All contents are Copyright © 1992–2005 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: May 23, 2005

Document ID: 64909
