

Cisco Security Response: Vulnerability in Java Secure Socket Extension

<http://www.cisco.com/warp/public/707/cisco-sr-20070725-jsse.shtml>

Revision 1.2

Last Updated 2008 June 30 1930 UTC (GMT)

For Public Release 2007 July 25 1600 UTC (GMT)

Please provide your [feedback](#) on this document.

Contents

[Cisco Response](#)

[Additional Information](#)

[Revision History](#)

[Cisco Security Procedures](#)

Cisco Response

This is the Cisco PSIRT response to the vulnerability in Java Secure Socket Extension (JSSE) disclosed by Sun Microsystems on July 10, 2007, the details of which are available at <http://sunsolve.sun.com/search/document.do?assetkey=1-26-102997-1>.

There are no workarounds available for this vulnerability. Cisco recommends that customers update all vulnerable applications and components to provide the greatest protection from the listed vulnerability.

Cisco will update this document in the event of any changes.

Additional Information

Some versions of Sun JSSE do not properly handle certain Transport Layer Security (TLS) or Secure Sockets Layer (SSL) handshake requests. A device running an affected JSSE version will experience excessive CPU usage, which may affect normal device operation and result in a denial of service (DoS) condition.

Sun has provided a comprehensive list of affected JSSE versions at the previously listed URL. Please refer to the Sun Alert Notification for details.

Products Affected by the JSSE Vulnerability

Note: The following list is subject to change. Cisco is continuing to review the potential impact of this vulnerability on its products; this list may be updated to include additional Cisco products that are affected by this vulnerability.

The following products are affected by the Sun JSSE issue listed in this Security Response:

- Cisco Unified Call Manager-Cisco bug ID is [CSCsh63934](#) ([registered](#) customers only) . Fixed software is available in releases 5.1(2) and 6.0(1). Customers running release 5.0 are advised to migrate to release 5.1(2) or later. Releases before 5.0 are not affected.
- Cisco Unified Presence-Cisco bug ID is [CSCsi77690](#) ([registered](#) customers only) . Fixed software is available in release 6.0(1). Customers running earlier versions are advised to migrate to release 6.0(1) or later.
- Cisco Unity Connection bug id is CSCsi79795 (registered customers only). Fixed software is available in release 2.0(1). Customers running earlier versions are advised to migrate to release 2.0(1) or later.

Workarounds

There is no workaround for this issue, but mitigation is possible.

Cisco Unified CallManager and Cisco Unified Presence customers are advised to restrict access to the administrative interface to the IP addresses of known management stations. Information on how to implement such access restrictions is available at the following link: http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/6x/security.html

Revision History

Revision 1.2	2008-June-30	Added information about Cisco Unity Connection
Revision 1.1	2007-July-26	Minor typo correction
Revision 1.0	2007-July-25	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>.

Help us help you.

Please rate this document.

- Excellent
- Good
- Average
- Fair
- Poor

This document solved my problem.

- Yes
- No
- Just browsing

Suggestions for improvement:

(256 character limit)



[Home](#)[How to Buy](#)[Login](#)[Profile](#)[Feedback](#)[Site Map](#)[Help](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 - 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)