Cisco Security Advisory

Open Query Interface in Cisco Unified Communications Manager and Cisco Unified Presence Server

Severity

Advisory ID: cisco-sa-20110824-cucm-cups
Last Updated: 2011 August 26 22:00 GMT
Published: 2011 August 24 16:00 GMT
Version1.1: Final
Workarounds: See below

Download CVRF
Download PDF
Email

Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the Security Vulnerability Policy. This document also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

Subscribe to Cisco Security Notifications

Subscribe

Summary

Cisco Unified Communications Manager (previously known as Cisco CallManager) and Cisco Unified Presence Server contain an open query interface that could allow an unauthenticated, remote attacker to disclose the contents of the underlying databases on affected product versions.

Cisco has released free updated software for most supported releases. A security patch file is also available for all supported versions that will remediate this issue. The patch may be applied to active systems without requiring a reload. Customers are advised to apply a fixed version or upgrade to a fixed train. Customers who need to stay on a version for which updated software is not currently available or who can not immediately apply the update are advised to apply the patch.

No workarounds are available for this issue.

This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110824-cucm-cups.

Affected Products

The following products are affected by the vulnerability described in this advisory:

Vulnerable Products

Cisco Unified Communications Manager

- Cisco Unified Communications Manager 6.x
- Cisco Unified Communications Manager 7.x
- Cisco Unified Communications Manager 8.0
- Cisco Unified Communications Manager 8.5

Note: Cisco Unified Communications Manager version 5.1 reached end of software maintenance on February 13, 2010. Customers who are using Cisco Unified Communications Manager 5.x versions should contact their Cisco support team for assistance in upgrading to a supported version of Cisco Unified Communications Manager.

Cisco Unified Presence Server

- Cisco Unified Presence Server 6.x
- Cisco Unified Presence Server 7.x
- Cisco Unified Presence Server 8.0
- Cisco Unified Presence Server 8.5

Products Confirmed Not Vulnerable

No other Cisco products are currently known to be affected by these vulnerabilities.

The following products are not affected by this vulnerability:

- Cisco Unified Communications Manager 4.x
- Cisco Unified Communications Manager 8.6(1x)
- Cisco Unified Presence Server 8.6(1x)
- Cisco Unity Connection
- Cisco Emergency Responder
- Cisco Unified Communications Manager Business Edition 3000
- Cisco Unified Communications Manager Business Edition 5000
- Cisco Unified Communications Manager Business Edition 6000

No other Cisco products are known to be affected by this vulnerability.

Details

Cisco Unified Communications Manager is the call processing component of the Cisco IP Telephony solution that extends enterprise telephony features and functions to packet telephony network devices such as IP phones, media processing devices, VoIP gateways, and multimedia applications.

Cisco Unified Presence Server is a standards-based enterprise platform that brings people together in and across organizations. This open and extensible platform facilitates the secure exchange of availability and instant messaging (IM) information between Cisco Unified Communications Manager and other applications.

Open Query Interface

Cisco Unified Communications Manager and Cisco Unified Presence Server contain an open query interface that could allow an unauthenticated, remote attacker to disclose some or all of the data contained in the underlying databases. This data may include authentication credentials, configuration details, and other sensitive information.

To exploit this issue, an attacker must have the ability to open an SSL connection to an affected device via TCP ports 443 or 8443. A completed three-way TCP handshake is required to exploit this vulnerability.

This vulnerability has been assigned CVE identifier CVE-2011-1643. The vulnerability is documented in the following Cisco BugIDs:

- **Cisco Unified Communications Manager - CSCti81574 (registered customers only)**
- **Cisco Unified Communications Manager - CSCto63060 (registered customers only)**
- **Cisco Unified Communications Manager - CSCto72183 (registered customers only)**

Cisco Unified Presence Server - CSCto73833 (registered customers only

Workarounds

There are no known workarounds for this issue.

Additional mitigations that can be deployed on Cisco devices within the network are available in the Cisco Applied Intelligence companion document for this advisory:

http://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20110824-cucm-cups

Fixed Software

When considering software upgrades, also consult http://www.cisco.com/go/psirt and any subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, contact the Cisco Technical Assistance Center (TAC) or your contracted maintenance provider for assistance.

Cisco Unified Communications Manager Version	First Fixed Release
6.x	Apply COP File
7.x	7.1(5b)su4 or Apply COP File
8.0	Apply COP File

8.5	8.5(1)su2 or Apply COP File
8.6	Not Affected

Note: The Cisco Unified Communications Manager Security COP file is available for download from the Cisco Software Center.

Cisco Unified Presence Server	First Fixed Release
6.x	Migrate to 8.5(4) or later or 8.6(x)
7.x	Apply COP File or Migrate to 8.5(4) or later or 8.6(x)
8.0	Apply COP File or Migrate to 8.5(4) or later or 8.6(x)
8.5	8.5(4)
8.6	Not Affected

Note: A Cisco Unified Presence Server patch in the form of a Security COP file is available via TAC for versions that do not currently have a published fixed version.

Exploitation and Public Announcements

The Cisco PSIRT is not aware of any public exploitation of the vulnerability described in this advisory.

This vulnerability was reported to Cisco by kxlzx.

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110824-cucm-cups

---

Revision History

Revision 1.1	2011-August-26	Updated version naming of 8.5xnr to 8.5(4) for clarification purposes.
Revision 1.0	2011-August-24	Initial public release.

Legal Disclaimer