Cisco Security Advisory

Cisco Unified Communications Manager Directory Traversal Vulnerability

High

Advisory ID:	cisco-sa-20111026-cucm
Last Updated:	2011 October 26 17:41 GMT
Published:	2011 October 26 16:00 GMT
Version1.1:	Final
CVSS Score:	Base - 7.8
Workarounds:	See below
Cisco Bug IDs:	CSCth09343 CSCts44049

CVE-2011-3315

Download CVRF
Download PDF
Email

Summary

Cisco Unified Communications Manager contains a directory traversal vulnerability that may allow an unauthenticated, remote attacker to retrieve arbitrary files from the filesystem.

Cisco has released software updates that address this vulnerability.

There are no workarounds that mitigate this vulnerability.

This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20111026-cucm.

Cisco Unified Contact Center Express and Cisco Unified IP Interactive Voice Response are also affected by this vulnerability, and a separate advisory has been published at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20111026-uccx.

Note: Effective October 18, 2011, Cisco moved the current list of Cisco Security Advisories and Responses published by Cisco PSIRT. The new location is http://tools.cisco.com/security/center/publicationListing. You can also navigate to this page from the Cisco Products and Services menu of the Cisco Security (SIO) Portal. Following this transition, new Cisco Security Advisories and Responses will be published to the new location. Although the URL has changed, the content of security documents and the vulnerability policy are not impacted. Cisco will continue to disclose security vulnerabilities in accordance with the published Security Vulnerability Policy.

Affected Products

Vulnerable Products

The following products are affected by this vulnerability:

- Cisco Unified Communications Manager 6.x
- Cisco Unified Communications Manager 7.x
- Cisco Unified Communications Manager 8.x

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.

Products Confirmed Not Vulnerable

Cisco Unified Communications Manager 4.x is not affected by this vulnerability.

With the exception of the Cisco Unified Contact Center Express and Cisco Unified IP Interactive Voice Response, no other Cisco products are currently 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 Communications Manager and Cisco Unified Contact Center Express Directory Traversal Vulnerability

Cisco Unified Communications Manager, Cisco Unified Contact Center Express and Cisco Unified IP Interactive Voice Response contain a directory traversal vulnerability that may allow an unauthenticated, remote attacker to retrieve arbitrary files from the filesystem.

Note: The Cisco Unified Communications Manager web service runs on port 8080.

This advisory addresses the vulnerability in Cisco Unified Communications Manager and is documented in Cisco bug ID CSCth09343 (registered customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) ID CVE-2011-3315.

Workarounds

There are no workarounds for this vulnerability.

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-20111026-cucm-uccx

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 Releases
6.x	6.1(5)SU2
7.x	7.1(5b)SU2
8.0	8.0(3)
8.5	Not vulnerable
8.6	Not vulnerable

Exploitation and Public Announcements

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerability described in this advisory.

This vulnerability was reported to Cisco by Felix "FX" Lindner of Recurity Labs.

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20111026-cucm

---

Revision History

Revision 1.1	2011-October-26	Corrected AMB URL.
Revision 1.0	2011-October-26	Initial public release.

Legal Disclaimer

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.

Related Resources

SA Cisco Unified Contact Center Express Directory Traversal Vulnerability

IS Cisco Unified Communications Manager and Unified Contact Center Express File Retrieval Directory Traversal Vulnerability

AMB Identifying and Mitigating Exploitation of the Cisco Unified Communications Manager and Cisco Unified Contact Center Express Directory Traversal Vulnerabilities

ST 39185

ST 39186

ST 39187

IPS Cisco Unified Communications Manager Directory Traversal Vulnerability

IPS Cisco Unified Contact Center Express Directory Traversal

IPS Cisco Unified Contact Center Express Directory Traversal

Subscribe to Cisco Security Notifications

Subscribe