Cisco Security Advisory

Cisco Unified Contact Center Express Directory Traversal Vulnerability

High

Advisory ID:	cisco-sa-20111026-uccx
Published:	2011 October 26 16:00 GMT
Version1.0:	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 Contact Center Express (UCCX or Unified CCX) and Cisco Unified IP Interactive Voice Response (Unified IP-IVR) contain a directory traversal vulnerability that may allow a remote, unauthenticated 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-uccx.

Cisco Unified Communications Manager is also affected by this vulnerability and a separate advisory has been published at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20111026-cucm.

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 Cisco UCCX versions are vulnerable:

- Cisco UCCX version 6.0(x)
- Cisco UCCX version 7.0(x)
- Cisco UCCX version 8.0(x)
- Cisco UCCX version 8.5(x)

Note: Cisco UCCX versions prior to 6.0(x) reached end of software maintenance. Customers running versions prior to 6.0(x) should contact their Cisco support team for assistance in upgrading to a supported version of Cisco UCCX.

The following Cisco Unified IP Interactive Voice Response versions are vulnerable:

- Cisco Unified IP Interactive Voice Response version 6.0(x)
- Cisco Unified IP Interactive Voice Response version 7.0(x)
- Cisco Unified IP Interactive Voice Response version 8.0(x)
- Cisco Unified IP Interactive Voice Response version 8.5(x)

Note: Cisco Unified IP Interactive Voice Response versions prior to 6.0(x) reached end of software maintenance. Customers running versions prior to 6.0(x) should contact their Cisco support team for assistance in upgrading to a supported version of Cisco Unified IP Interactive Voice Response.

Products Confirmed Not Vulnerable

With the exception of Cisco Unified Communications Manager, no other Cisco products are currently known to be affected by this vulnerability.

Details

The Cisco Unified Contact Center Express is a single/two node server, integrated "contact center in a box" for use in deployments with up to 300 agents until software version 8.0(x) and 400 agents starting at version 8.5(x).

The Cisco Unified Interactive Voice Response is a UCCX product package that provides IP call queuing and IP intelligent voice response functionality for contact centers.

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.

The vulnerability is due to improper input validation, and could allow the attacker to traverse the filesystem directory. An attacker could exploit this vulnerability by sending a specially crafted URL to the affected system.

The vulnerability in Cisco Unified Contact Center Express and Cisco Unified IP Interactive Voice Response could be exploited over TCP port 8080 in 6.0(x) and 7.0(x) versions and TCP port 9080 starting in 8.0(x) version of the product.

Note: In Cisco Unified Contact Center Express and Cisco Unified IP Interactive Voice Response versions 6.0(x) and 7.0(x), port 8080 could be reconfigured on the server.

This advisory addresses the vulnerability in Cisco Unified Contact Center Express and Cisco Unified IP Interactive Voice Response, which is documented in Cisco bug ID CSCts44049 (registered customers only) and has been assigned 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

Cisco has released software updates that address this vulnerability.

The following table contains the remediation for each affected version of Cisco Unified Contact Center Express and Cisco Unified IP Interactive Voice Response:

Version	First Fixed in
6.0(x)	6.0(1)SR1ES8
7.0(x)	7.0(2)ES1
8.0(x)	8.0(2)SU3 and patch ciscouccx.802SU3_CSCts44049.cop.sgn
8.5(x)	8.5(1)SU2

Releases 6.0(1)SR1ES8 and 7.0(2)ES1 will not be posted on cisco.com. Customers should contact Cisco Technical Assistance Center (TAC) for assistance.

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.

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 the Vulnerability Research Team of Digital Defense, Inc.

URL

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

---

Revision History

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 Communications Manager 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

Revision 1.0	2011-October-26	Initial public release

Legal Disclaimer

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

A stand-alone copy or paraphrase of the text of this document that omits the distribution URL is an uncontrolled copy, and may lack important information or contain factual errors. The information in this document is intended for end-users of Cisco products.