Cisco Security Advisory

Cisco Unified Communications Manager IPMA Cross-Site Scripting Vulnerability

Medium

Advisory ID:	Cisco-SA-20140212-CVE-2014-0723
Published:	2014 February 12 17:40 GMT
Version1.0:	Final
CVSS Score:	Base - 4.3
Workarounds:	See below
Cisco Bug IDs:	CSCum05343

CVE-2014-0723
CWE-79

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

A vulnerability in the Cisco IP Manager Assistant (IPMA) interface of Cisco Unified Communications Manager (UCM) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web interface on the affected system.

The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by convincing a user to access a malicious link.

Cisco has confirmed the vulnerability in a security notice; however, software updates are not available.

To exploit the vulnerability, the attacker may provide a link that directs a user to a malicious site and use misleading language or instructions to persuade the user to follow the provided link.

Cisco indicates through the CVSS score that functional exploit code exists; however, the code is not known to be publicly available.

Affected Products

Customers are advised to consult Cisco bug ID CSCum05343 for the most complete list of affected product versions.

Vulnerable Products

At the time this alert was first published, Cisco UCM versions 10.0(1) and prior were vulnerable. Later releases of Cisco UCM may also be vulnerable.

Products Confirmed Not Vulnerable

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

Workarounds

Administrators are advised to contact the vendor regarding future updates and releases.

Users are advised not to visit websites or follow links that have suspicious characteristics or cannot be verified as safe.

For additional information about cross-site scripting attacks and the methods used to exploit these vulnerabilities, see the Cisco Applied Mitigation Bulletin Understanding Cross-Site Scripting (XSS) Threat Vectors.

Administrators may consider using IP-based access control lists (ACLs) to allow only trusted systems to access the affected systems.

Administrators are advised to monitor affected systems.

Fixed Software

Software updates are not available.

Exploitation and Public Announcements

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20140212-CVE-2014-0723

Revision History

Version	Description	Section	Status	Date
1.0	Initial Release	NA	Final	2014-Feb-12

Legal Disclaimer

Information For
Small Business
Midsize Business
Service Provider
Executives

Industries

Marketplace

Contacts
Contact Cisco
Find a Reseller

News & Alerts
Newsroom
Blogs
Field Notices
Security Advisories

Technology Trends
Cloud
Internet of Things (IoT)
Mobility
Software Defined Networking (SDN)

Support
Downloads
Documentation

Communities
DevNet
Learning Network
Support Community

Video Portal

About Cisco
Investor Relations
Corporate Social Responsibility
Environmental Sustainability
Tomorrow Starts Here
Our People

Careers
Search Jobs
Life at Cisco

Programs
Cisco Designated VIP Program
Cisco Powered
Financing Options

Contacts | Feedback | Help | Site Map | Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks