

Cisco Security Advisory

Cisco Unified Products Information Disclosure Vulnerability



Advisory ID: cisco-sa-20160208-ucm
Published: 2016 February 8 14:00 GMT
Version 1.0: Final
CVSS Score: [Base - 5.0](#)
Workarounds: No workarounds available
Cisco Bug IDs: [CSCuv85926](#)
[CSCuv85929](#)
[CSCuv85931](#)
[CSCuv85949](#)
[CSCuv85958](#)
[CSCuv85998](#)

[CVE-2016-1319](#) [Download CVRE](#)
[CWE-200](#) [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 key management feature of multiple Cisco Unified products could allow an unauthenticated, local attacker to read sensitive data.

The vulnerability is due to an encryption key that can be read in plain text. An attacker could exploit this vulnerability by determining the key and decrypting certain data sets. An exploit could allow the attacker to read and disclose sensitive data.

Cisco released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

This advisory is available at the following link:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160208-ucm>

Affected Products

Vulnerable Products

At the time this advisory was first published, the following Cisco products were vulnerable:

- Cisco Unified Communications Manager (CallManager) Releases 10.5(2.12901.1), 10.5(2.10000.5), 11.0(1.10000.10), and 9.1(2.10000.28)
- Cisco Unified Communications Manager IM Presence Service Release 10.5(2)
- Cisco Unified Contact Center Express Release 11.0(1)
- Cisco Unity Connection Release 10.5(2)

Products Confirmed Not Vulnerable

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

Workarounds

There are no workarounds that address this vulnerability.

Fixed Software

When considering software upgrades, customers are advised to consult the Cisco Security Advisories and Responses archive at <http://www.cisco.com/go/psirt> and review subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should ensure that the devices to upgrade contain sufficient memory and confirm that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, customers are advised to contact the Cisco Technical Assistance Center (TAC) or their contracted maintenance providers.

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-20160208-ucm>

Revision History

Version	Description	Section	Status	Date
1.0	Initial public release.	-	Final	2016-February-08

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 standalone 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.

Information For

[Small Business](#)
[Midsized 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](#)