Cisco Security Advisory

# Cisco Unified Communications Manager Memory Leak Vulnerability

Severity

**Advisory ID:** cisco-sa-20110928-cucm
**Last Updated:** 2012 July 18 14:05 GMT
**Published:** 2011 September 28 16:00 GMT
**Version1.1:** Final
**Workarounds:** See below
**Cisco Bug IDs:** CSCtl86047

CVE-2011-2072

Download CVRF
Download PDF
Email



**Summary**

Cisco Unified Communications Manager contains a memory leak vulnerability that could be triggered through the processing of malformed Session Initiation Protocol (SIP) messages. Exploitation of this vulnerability could cause an interruption of voice services. Cisco has released free software updates for supported Cisco Unified Communications Manager versions to address the vulnerability. A workaround exists for this SIP vulnerability.

This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-cucm.

**Note:** The September 28, 2011, Cisco IOS Software Security Advisory bundled publication includes ten Cisco Security Advisories. Nine of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses a vulnerability in Cisco Unified Communications Manager. Each advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all vulnerabilities in the September 2011 Bundled Publication.

Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep11.html

Cisco IOS Software is affected by the SIP vulnerability described in this advisory. A separate Cisco Security Advisory has been published to disclose the vulnerabilities that affect the Cisco IOS software at the following location: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-sip.

## Affected Products

### Vulnerable Products

The following products are affected by vulnerabilities that are described in this advisory:

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

**Note:** Cisco Unified Communications Manager version 6.1 reached the End of Software Maintenance on September 3, 2011. Customers using Cisco Unified Communications Manager 6.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 version 4.x is not affected by this vulnerability. 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.**

**Memory Leak Vulnerability in SIP**

**Cisco Unified Communications Manager contains a vulnerability that involves the processing of SIP messages. Cisco Unified Communications Manager may leak session control buffers (SCBs) or cause a reload of the affected device when processing a malformed SIP message. Exploitation of the vulnerability may cause a critical process to fail, which could result in the disruption of voice services. All SIP ports (TCP ports 5060 and 5061 and UDP ports 5060 and 5061) are affected.**

**This SIP vulnerability is documented in Cisco Bug ID CSCtl86047 (registered customers only) and has been assigned the CVE identifier CVE-2011-2072. This vulnerability is fixed in Cisco Unified Communications Manager versions 8.6(1), 8.5(1)su2, and 7.1(5b)su4. [Note, there is not a software Service Update for the 6.x version that contains the fix.]**

**Note: This vulnerability also affects Cisco IOS Software. The corresponding Cisco Bug ID is CSCto88686. Refer to the separate Cisco Security Advisory for the Cisco IOS Software for additional details.**

## Workarounds

A workaround exists for customers who do not require SIP in their environment. Cisco Unified Communication Manager versions 6.1(4), 7.1(2) and 8.0(1) introduced the ability to disable SIP processing. SIP processing is enabled by default. Use the following instructions to disable SIP processing:

- **Step 1:** Log in to the Cisco Unified CM Administration web interface.
- **Step 2:** Navigate to **System Service Parameters** and select the appropriate Cisco Unified Communications Manager server and the Cisco CallManager service.
- **Step 3:** Change the SIP Interoperability Enabled parameter to False and click **Save.**

  **Note:** For a SIP processing change to take effect, the Cisco CallManager Service must be restarted. For information on how to restart the service, refer to the "Restarting the Cisco CallManager Service" section of the document at http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/7_1_2/ccmcfg/b03dpi.html#wp1075124

  It is possible to mitigate these vulnerabilities by implementing filtering on screening devices and permitting access to TCP ports 5060 and 5061 and UDP ports 5060 and 5061 only from networks that require SIP access to Cisco Unified Communications Manager servers.
  Additional mitigations that can be deployed on Cisco devices in the network are available in the companion document "Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Multiple Vulnerabilities in Cisco Voice Products" which is available at the following location:
  http://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20110928-voice

## 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. Cisco recommends upgrading to a release equal to or later than the release in the "Recommended Releases" column of the table.

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.

Additionally, the Cisco IOS Software Checker is available on the Cisco Security (SIO) portal at http://tools.cisco.com/security/center/selectIOSVersion.x. It provides several features for checking which Security Advisories affect specified versions of Cisco IOS Software.

| Cisco Unified Communication Manager Version | Recommended Release |
|---|---|
| 7.x | 7.1(5b)su4 |
| 8.x* | 8.5(1)su2, 8.6(1) |

*The recommended releases listed in the table above are the latest Cisco Unified Communications Manager versions available at the publication of this advisory. Software updates for 6.1 and 8.0 are not available for CSCtl86047. Customers using these versions should consult their Cisco support team for assistance in upgrading to a supported release.

Cisco Unified Communications Manager software can be downloaded from the following link:
http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=268439621

## 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 found during internal testing and the troubleshooting of customer service requests.

**URL**

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-cucm

---

**Revision History**

| | | |
|---|---|---|
| Revision 1.1 | 2012-July-17 | Updated meta-tags |
| Revision 1.0 | 2011-September-28 | Initial public release. |

---