

Cisco Security Advisory: Cisco Unified Communications Manager Express Vulnerability

Advisory ID: cisco-sa-20090923-cme

<http://www.cisco.com/warp/public/707/cisco-sa-20090923-cme.shtml>

Revision 1.0

For Public Release 2009 September 23 1600 UTC (GMT)

Please provide your [feedback](#) on this document.

Contents

[Summary](#)

[Affected Products](#)

[Details](#)

[Vulnerability Scoring Details](#)

[Impact](#)

[Software Versions and Fixes](#)

[Workarounds](#)

[Obtaining Fixed Software](#)

[Exploitation and Public Announcements](#)

[Status of this Notice: FINAL](#)

[Distribution](#)

[Revision History](#)

[Cisco Security Procedures](#)

Summary

Cisco IOS® devices that are configured for Cisco Unified Communications Manager Express (CME) and the Extension Mobility feature are vulnerable to a buffer overflow vulnerability. Successful exploitation of this vulnerability may result in the execution of arbitrary code or a Denial of Service (DoS) condition on an affected device.

Cisco has released free software updates that address this vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-cme.shtml>.

Note: The September 23, 2009, Cisco IOS Security Advisory bundled publication includes eleven Security Advisories. Ten of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses a vulnerability in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory.

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

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep09.html

[\[Expand all sections\]](#) [\[Collapse all sections\]](#)

☐ Affected Products

Cisco IOS devices, including Cisco Unified Communications 500 Series, that are configured for Cisco Unified CME and the Extension Mobility feature are affected.

☐ Vulnerable Products

A Cisco IOS device that is configured for Cisco Unified CME and Extension Mobility contains the following output when the **show running-config** command is issued:

```
ephone [Ethernet phone tag]
...
logout-profile [logout-profile tag]
```

To determine the Cisco IOS Software release that is running on a Cisco product, administrators can log in to the device and issue the **show version** command to display the system banner. The

system banner confirms that the device is running Cisco IOS Software by displaying text similar to "Cisco Internetwork Operating System Software" or "Cisco IOS Software." The image name is displayed in parentheses, followed by "Version" and the Cisco IOS Software release name. Other Cisco devices do not have the **show version** command or may provide different output.

The following example identifies a Cisco product that is running Cisco IOS Software Release 12.3(26) with an installed image name of C2500-IS-L:

```
Router#show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-IS-L), Version 12.3
(26), RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by cisco Systems, Inc.
Compiled Mon 17-Mar-08 14:39 by dchih

<output truncated>
```

The following example identifies a Cisco product that is running Cisco IOS Software Release 12.4(20)T with an installed image name of C1841-ADVENTERPRISEK9-M:

```
Router#show version
Cisco IOS Software, 1841 Software (C1841-
ADVENTERPRISEK9-M), Version 12.4(20)T, RELEASE
SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team

<output truncated>
```

Additional information about Cisco IOS Software release naming conventions is available in "White Paper: Cisco IOS Reference Guide" at the following link: <http://www.cisco.com/warp/public/620/1.html>.

☐ Products Confirmed Not Vulnerable

Cisco IOS devices that are configured for Survivable Remote Site Telephony (SRST) Mode are not affected.

Cisco IOS XR is not affected.

Cisco IOS XE is not affected.

Cisco Unified Communications Manager is not affected.

Cisco Unified CME is not affected unless configured to use the Extension Mobility feature.

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

[Top of the section](#) [Close Section](#)

☐ Details

Cisco Unified CME is the call processing component of an enhanced IP telephony solution that is integrated into Cisco IOS.

The Extension Mobility feature in Cisco Unified CME provides the benefit of phone mobility for end users. A user login service allows phone users to temporarily access a physical phone other than their own phone and utilize their personal settings, such as directory number, speed-dial lists, and services, that is assigned to their own desk phone. The phone user can make and receive calls on that phone using the same personal directory number as is on their own desk phone. More information on Extension Mobility feature is available at the following URL:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmemobl.html

A vulnerability in the login section of the Extension Mobility feature may allow an unauthenticated attacker to execute arbitrary code or cause a Denial of Service (DoS) condition. Such packets can only come from registered phone IP addresses in the form of HTTP requests. If the auto-registration feature is enabled, an attacker can register its IP address and subsequently send a crafted payload to exploit this vulnerability. The auto-registration feature is enabled by default. More information on auto-registration can be found at the following link:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/command/reference/cme_a1.html#wp1031242.

This vulnerability is addressed by the Cisco Bug ID [CSCsq58779](#) ([registered](#) customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) ID CVE-2009-2865.

☐ Vulnerability Scoring Details

Cisco has provided scores for the vulnerabilities in this advisory based on the Common Vulnerability Scoring System (CVSS). The CVSS scoring in this Security Advisory is done in accordance with CVSS version 2.0.

CVSS is a standards-based scoring method that conveys vulnerability severity and helps determine urgency and priority of response.

Cisco has provided a base and temporal score. Customers can then compute environmental scores to assist in determining the impact of the vulnerability in individual networks.

Cisco has provided an FAQ to answer additional questions regarding CVSS at

<http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html> .

Cisco has also provided a CVSS calculator to help compute the environmental impact for individual networks at

<http://intellishield.cisco.com/security/alertmanager/cvss> .

CSCsq58779 - Vulnerability in Extension Mobility Feature					
Calculate the environmental score of Calculate the environmental score of Bug ID CVSS scoring link					
CVSS Base Score - 7.6					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	High	None	Complete	Complete	Complete
CVSS Temporal Score - 6.3					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

☐ Impact

Successful exploitation of this vulnerability may result in the execution of arbitrary code or a Denial of Service (DoS) condition on an affected device.

[Top of the section](#) [Close Section](#)

☐ Software Versions and Fixes

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.

Each row of the Cisco IOS software table (below) names a Cisco IOS release train. If a given release train is vulnerable, then the earliest possible releases that contain the fix (along with the anticipated date of availability for each, if applicable) are listed in the "First Fixed Release" column of the table. The "Recommended Release" column indicates the releases which have fixes for all the published vulnerabilities at the time of this Advisory. A device running a release in the given train that is earlier than the release in a specific column (less than the First Fixed Release) is known to be vulnerable. Cisco recommends upgrading to a release equal to or later than the release in the "Recommended Releases" column of the table.

Major Release	Availability of Repaired Releases	
Affected 12.0-Based Releases	First Fixed Release	Recommended Release
There are no affected 12.0 based releases.		

Affected 12.1- Based Releases	First Fixed Release	Recommended Release
-------------------------------------	------------------------	------------------------

There are no affected 12.1 based releases.

Affected 12.2- Based Releases	First Fixed Release	Recommended Release
-------------------------------------	------------------------	------------------------

There are no affected 12.2 based releases.

Affected 12.3- Based Releases	First Fixed Release	Recommended Release
-------------------------------------	------------------------	------------------------

There are no affected 12.3 based releases.

Affected 12.4- Based Releases	First Fixed Release	Recommended Release
-------------------------------------	------------------------	------------------------

12.4

Not Vulnerable

12.4GC

Not Vulnerable

12.4JA

Not Vulnerable

12.4JDA

Not Vulnerable

12.4JDC

Not Vulnerable

12.4JDD

Not Vulnerable

12.4JK

Not Vulnerable

12.4JL	Not Vulnerable	
12.4JMA	Not Vulnerable	
12.4JMB	Not Vulnerable	
12.4JX	Not Vulnerable	
12.4MD	Not Vulnerable	
12.4MDA	Not Vulnerable	
12.4MR	Not Vulnerable	
12.4SW	Not Vulnerable	
12.4T	Not Vulnerable	
12.4XA	Not Vulnerable	
12.4XB	Not Vulnerable	
12.4XC	Not Vulnerable	
12.4XD	Not Vulnerable	
12.4XE	Not Vulnerable	
12.4XF	Not Vulnerable	
12.4XG	Not Vulnerable	

12.4XJ	Not Vulnerable	
12.4XK	Not Vulnerable	
12.4XL	Not Vulnerable	
12.4XM	Not Vulnerable	
12.4XN	Not Vulnerable	
12.4XP	Not Vulnerable	
12.4XQ	Not Vulnerable	
12.4XR	Not Vulnerable	
12.4XT	Not Vulnerable	
12.4XV	Not Vulnerable	
12.4XW	12.4(11)XW8	12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4XY	12.4(15)XY4	12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009

12.4XZ	12.4(15)XZ1	12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4YA	12.4(20)YA1	12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4YB	Not Vulnerable	
12.4YD	Not Vulnerable	
12.4YE	Not Vulnerable	

[Top of the section](#) [Close Section](#)

☐ Workarounds

There are no workarounds to mitigate this vulnerability, other than disabling Extension Mobility. However, auto-registration can be disabled to make exploitation more difficult. Auto-registration can be disabled by the following command:

```
telephony-service
  no auto-reg-ephone
```

Before disabling auto-registration, all phone MAC addresses need to be explicitly defined on the Cisco Unified CME. Otherwise phones will not be able to register. More information on auto-registration can be found at the following link:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/command/reference/cme_al.html#wp1031242

Additional mitigations that can be deployed on Cisco devices in the network are available in the

Cisco Applied Mitigation Bulletin companion document for this advisory, which is available at the following link: <http://www.cisco.com/warp/public/707/cisco-amb-20090923-cme.shtml>

[Top of the section](#) [Close Section](#)

☐ **Obtaining Fixed Software**

Cisco has released free software updates that address this vulnerability. Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

Customers may only install and expect support for the feature sets they have purchased. By installing, downloading, accessing or otherwise using such software upgrades, customers agree to be bound by the terms of Cisco's software license terms found at http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact psirt@cisco.com or security-alert@cisco.com for software upgrades.

☐ **Customers with Service Contracts**

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's worldwide website at <http://www.cisco.com>.

☐ **Customers using Third Party Support Organizations**

Customers whose Cisco products are provided or maintained through prior or existing agreements with third-party support organizations, such as Cisco Partners, authorized resellers, or service providers should contact that support organization for guidance and assistance with the appropriate course of action in regards to this advisory.

The effectiveness of any workaround or fix is dependent on specific customer situations, such as product mix, network topology, traffic behavior, and organizational mission. Due to the variety of affected products and releases, customers should consult with their service provider or support organization to ensure any applied workaround or fix is the most appropriate for use in the intended network before it is deployed.

☐ **Customers without Service Contracts**

Customers who purchase direct from Cisco but do not hold a Cisco service contract, and customers who purchase through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should acquire upgrades by contacting the Cisco Technical Assistance Center (TAC). TAC contacts are as follows.

- +1 800 553 2447 (toll free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)
- e-mail: tac@cisco.com

Customers should have their product serial number available and be prepared to give the URL of this notice as evidence of entitlement to a free upgrade. Free upgrades for non-contract customers must be requested through the TAC.

Refer to http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html for additional TAC contact information, including localized telephone numbers, and instructions and e-mail addresses for use in various languages.

[Top of the section](#) [Close Section](#)

☐ **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 internally.

[Top of the section](#) [Close Section](#)

☐ **Status of this Notice: FINAL**

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 in the following section is an uncontrolled copy, and may lack important information or contain factual errors.

☐ Distribution

This advisory is posted on Cisco's worldwide website at :

<http://www.cisco.com/warp/public/707/cisco-sa-20090923-cme.shtml>

In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key and is posted to the following e-mail and Usenet news recipients.

- cust-security-announce@cisco.com
- first-bulletins@lists.first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- comp.dcom.sys.cisco@newsgate.cisco.com

Future updates of this advisory, if any, will be placed on Cisco's worldwide website, but may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the above URL for any updates.

☐ Revision History

Revision 1.0	2009-September-23	Initial public release
--------------	-------------------	------------------------

☐ Cisco Security Procedures

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html. This includes instructions for press inquiries regarding

Help us help you.



Please rate this document.

- Excellent
- Good
- Average
- Fair
- Poor



This document solved my problem.

- Yes
- No
- Just browsing



Suggestions for improvement:

(256 character limit)



[Home](#)

[How to Buy](#)

[Login](#)

[Profile](#)

[Feedback](#)

[Site Map](#)

[Help](#)