

Cisco Security Advisory: Cisco Unified Communications Manager IP Phone Personal Address Book Synchronizer Privilege Escalation Vulnerability

Advisory ID: cisco-sa-20090311-cucmpab

<http://www.cisco.com/warp/public/707/cisco-sa-20090311-cucmpab.shtml>

Revision 1.0

For Public Release 2009 March 11 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](#)

Summary

Cisco Unified Communications Manager, formerly CallManager, contains a privilege escalation vulnerability in the IP Phone Personal Address Book (PAB) Synchronizer feature that may allow an attacker to gain complete administrative access to a vulnerable Cisco Unified Communications Manager system. If Cisco Unified Communications Manager is integrated with an external directory service, it may be possible for an attacker to leverage the privilege escalation vulnerability to gain access to additional systems configured to use the directory service for authentication.

Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090311-cucmpab.shtml>.

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

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

☐ Affected Products

☐ Vulnerable Products

The following products are vulnerable:

- Cisco Unified CallManager 4.1 versions
- Cisco Unified Communications Manager 4.2 versions prior to 4.2(3)SR4b
- Cisco Unified Communications Manager 4.3 versions prior to 4.3(2)SR1b
- Cisco Unified Communications Manager 5.x versions prior to 5.1(3e)
- Cisco Unified Communications Manager 6.x versions prior to 6.1(3)
- Cisco Unified Communications Manager 7.0 versions prior to 7.0(2)

Administrators of systems that are running Cisco Unified Communications Manager software version 4.x can determine the software version by navigating to **Help > About Cisco Unified CallManager** and selecting the **Details** button via the Cisco Unified Communications Manager administration interface.

Administrators of systems that are running Cisco Unified Communications Manager software

versions 5.x, 6.x, and 7.x can determine the software version by viewing the main page of the Cisco Unified Communications Manager administration interface. The software version can also be determined by running the command **show version active** via the command line interface (CLI).

☐ **Products Confirmed Not Vulnerable**

Cisco Unified Communications Manager Express is not affected by this vulnerability. No other Cisco products are currently known to be affected by this vulnerability.

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

☐ **Details**

The Cisco IP Phone Personal Address Book (PAB) Synchronizer feature of Cisco Unified Communications Manager allows users to keep their Cisco Unified Communications Manager address book synchronized with their Microsoft Windows address book. The IP Phone PAB Synchronizer feature contains a privilege escalation vulnerability that may allow an attacker to obtain complete administrative access to a vulnerable Cisco Unified Communications Manager system. After an IP Phone PAB Synchronizer client successfully authenticates to a Cisco Unified Communications Manager device over a HTTPS connection, the Cisco Unified Communications Manager returns credentials for a user account that is used to manage the Cisco Unified Communications Manager directory service. If an attacker is able to intercept the credentials, they can perform unauthorized modifications to the Cisco Unified Communications Manager configuration and extend their privileges. The IP Phone PAB Synchronizer client has been redesigned to allow address book synchronization without requiring the directory service credentials. This vulnerability does not allow an attacker to gain access to the underlying platform operating system of any Cisco Unified Communications Manager system.

Cisco Unified Communications Manager 4.x

Cisco Unified Communications Manager software version 4.x by default stores user information using an internal Lightweight Directory Access Protocol (LDAP) server called DC Directory. After an IP Phone PAB Synchronizer client successfully authenticates, the Cisco Unified Communications Manager returns credentials for the DC Directory user that will be used by the client to synchronize a user's address book. Depending on how a Cisco Unified Communications Manager is configured, an attacker may obtain different privilege levels using the intercepted credentials.

By default, Cisco Unified Communications Manager software version 4.x administrator accounts are created as part of an underlying Microsoft Windows operating system. Cisco Unified Communications Manager is commonly deployed using the Multi-Level Administration (MLA)

feature to ease the integration of Cisco Unified Communications Manager into enterprise environments. If MLA is enabled, Cisco Unified Communications Manager stores administrator accounts in the Cisco Unified Communications Manager DC Directory service. If an attacker obtains the DC Directory credentials and MLA is enabled, the attacker can add an existing account to the Cisco Unified Communications Manager super-user group. The attacker can then access the Cisco Unified Communications Manager management interface with complete administrative access. If MLA is not enabled, the attacker cannot escalate their privileges; however, they can modify any user settings in the directory.

The Cisco Unified Communications Manager 4.x IP Phone PAB Synchronizer client uses an unencrypted LDAP connection to perform address book synchronization. The DC Directory credentials are passed in the clear over the network and are vulnerable to being sniffed by an attacker. If using the DC Directory internal LDAP server, the IP Phone PAB Synchronizer client communicates to Cisco Unified Communications Manager on TCP ports 8404 and 8405.

Cisco Unified Communications Manager 5.x, 6.x, 7.x

Cisco Unified Communications Manager software versions 5.x, 6.x, and 7.x store user information as a part of the internal Cisco Unified Communications Manager configuration database. The IP Phone PAB Synchronizer client uses the AXL application programming interface (API) to perform address book synchronization. After a client successfully authenticates, the Cisco Unified Communications Manager returns credentials for a database user account named TabSyncSysUser that will be used by the client to synchronize an user's address book. The TabSyncSysUser account has full read and write privileges to the Cisco Unified Communications Manager configuration database. Using the TabSyncSysUser credentials via the AXL API, an attacker can modify any parameter in the database including creating new administrator accounts.

Directory Service Integration

Cisco Unified Communications Manager software versions 4.x, 5.x, 6.x, and 7.x can be integrated with Microsoft Active Directory and several non-Microsoft LDAP servers to perform user authentication. In order to function properly, the integration process requires that appropriate user credentials for the directory service are provided to Cisco Unified Communications Manager. If an attacker intercepts or sniffs the directory service credentials returned by a Cisco Unified Communications Manager responding to an IP Phone PAB Synchronizer client, the attacker may be able to leverage the credentials to gain access to additional systems configured to use the directory service for authentication.

Administrators should ensure that any directory service credentials used for the Cisco Unified Communications Manager integration process are configured to follow the principle of least privilege. The credentials should be configured with only the privileges necessary to access the directory service data needed for the integration process to function properly. The use of overly

privileged administrator accounts is discouraged. Please see the Workarounds section for more information on performing the integration of Cisco Unified Communications Manager with AD using the least privilege concept.

This vulnerability is documented in Cisco Bug IDs CSCso76587 and CSCso78528 and has been assigned Common Vulnerabilities and Exposures (CVE) identifier CVE-2009-0632.

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

☐ Vulnerability Scoring Details

Cisco has provided scores for the vulnerability 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>

CSCso76587 - Directory Manager password sent in clear from client
(registered customers only)

Calculate the environmental score of CSCso76587

CVSS Base Score - 9

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
---------------	-------------------	----------------	------------------------	------------------	---------------------

Network	Low	Single	Complete	Complete	Complete
CVSS Temporal Score - 7.4					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

<u>CSCso78528 - TabSyncSysUser (axl user) password sent in clear from client (<u>registered</u> customers only)</u>					
Calculate the environmental score of <u>CSCso78528</u>					
CVSS Base Score - 9					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	Single	Complete	Complete	Complete
CVSS Temporal Score - 7.4					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

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

☐ Impact

Successful exploitation of this vulnerability may allow an attacker to intercept user credentials that allow the attacker to escalate their privilege level and obtain complete administrative access to a vulnerable Cisco Unified Communications Manager system. If integrated with an external directory service, the intercepted user credentials may allow an attacker to gain access to additional systems configured to use the directory service for authentication.

[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.

Cisco Unified Communications Manager software version 4.2(3)SR4b contains the fix for this vulnerability. Administrators of Cisco Unified CallManager software version 4.1 systems are encouraged to upgrade to Cisco Unified Communications Manager software version 4.2(3)SR4b in order to obtain fixed software. Version 4.2(3)SR4b can be downloaded at the following link:

<http://tools.cisco.com/support/downloads/go/PlatformList.x?sftType=Unified%20Communications%20Manager%20Updates&mdfid=280264388&treeName=Voice%20and%20Unified%20Communications&mdfLevel=Software%20Version/Option&url=null&modelName=Cisco%20Unified%20CallManager%20Version%204.2&isPlatform=N&treeMdfId=278875240&modifmdfid=null&imname=null&hybrid=Y&imst=N>

Cisco Unified Communications Manager software version 4.3(2)SR1b contains the fix for this vulnerability. Version 4.3(2)SR1b can be downloaded at the following link:

<http://tools.cisco.com/support/downloads/go/PlatformList.x?sftType=Unified%20Communications%20Manager%20Updates&mdfid=280771554&treeName=Voice%20and%20Unified%20Communications&mdfLevel=Software%20Version/Option&url=null&modelName=Cisco%20Unified%20Communications%20Manager%20Version%204.3&isPlatform=N&treeMdfId=278875240&modifmdfid=null&imname=null&hybrid=Y&imst=N>

Cisco Unified Communications Manager software version 5.1(3e) contains the fix for this vulnerability. Version 5.1(3e) can be downloaded at the following link:

<http://tools.cisco.com/support/downloads/go/ReleaseType.x?optPlat=null&isPlatform=Y&mdfid=280735907&sftType=Unified%20Communications%20Manager%20Updates&treeName=Voice%20and%20Unified%20Communications&modelName=Cisco%20Unified%20Communications%20Manager%20Version%205.1&mdfLevel=Software%20Version/Option&treeMdfId=278875240&modifmdfid=null&imname=null&hybrid=Y&imst=N>

Cisco Unified Communications Manager software version 6.1(3) contains the fix for this vulnerability. Version 6.1(3) can be downloaded at the following link:

<http://tools.cisco.com/support/downloads/go/PlatformList.x?sftType=Unified%20Communications%20Manager%20Updates&mdfid=280771554&treeName=Voice%20and%20Unified%20Communications&mdfLevel=Software%20Version/Option&url=null&modelName=Cisco%20Unified%20Communications%20Manager%20Version%206.1&isPlatform=N&treeMdfId=278875240&modifmdfid=null&imname=null&hybrid=Y&imst=N>

[20Manager%20Updates&mdfid=281023410&treeName=Voice%20and%20Unified%20Communications&mdfLevel=Software%20Version/Option&url=null&modelName=Cisco%20Unified%20Communications%20Manager%20Version%206.1&isPlatform=N&treeMdfId=278875240&modifmdfid=null&imname=null&hybrid=Y&imst=N](http://tools.cisco.com/support/downloads/go/ReleaseType.x?optPlat=&isPlatform=Y&mdfid=281941895&sftType=Unified+Communications+Manager+Updates&treeName=Voice+and+Unified+Communications&modelName=Cisco+Unified+Communications+Manager+Version+7.0&mdfLevel=Software%20Version/Option&treeMdfId=278875240&modifmdfid=null&imname=&hybrid=Y&imst=N)

Cisco Unified Communications Manager software version 7.0(2) contains the fix for this vulnerability. Version 7.0(2) can be downloaded at the following link:

<http://tools.cisco.com/support/downloads/go/ReleaseType.x?optPlat=&isPlatform=Y&mdfid=281941895&sftType=Unified+Communications+Manager+Updates&treeName=Voice+and+Unified+Communications&modelName=Cisco+Unified+Communications+Manager+Version+7.0&mdfLevel=Software%20Version/Option&treeMdfId=278875240&modifmdfid=null&imname=&hybrid=Y&imst=N>

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

☐ Workarounds

It is possible to mitigate against this vulnerability using the following workarounds.

Cisco Unified Communications Manager 4.x

It is possible to mitigate this vulnerability by moving the ASP script that IP Phone Personal Address Book (PAB) Scynchronizer clients interact with to a directory location that is not accessible to the Cisco Unified Communications Manager web server. The system drive where the ASP script resides depends on how Cisco Unified Communications Manager was installed. Employing this workaround will prevent address book synchronization; however, the PAB application will continue to function. The ASP script can be moved using the following command:

```
C:\> move c:\CiscoWebs\User\LDAPDetails.asp c:\temp
```

It is also possible to mitigate this vulnerability by implementing filtering on screening devices or using the Windows firewall. Administrators are advised to permit access to TCP ports 8404 and 8405 only from trusted networks.

Cisco Unified Communications Manager 5.x, 6.x, 7.x

It is possible to mitigate this vulnerability by restricting the permissions of the TabSyncSysUser database user account. In the Cisco Unified Communications Manager Administration interface, navigate to **User Management > Application User** and search for the TabSyncSysUser account.

Remove all groups from the account and change the password. Employing this workaround will prevent address book synchronization; however, the PAB application will continue to function.

Active Directory Integration

To improve the security of Cisco Unified Communications Manager integration with Active Directory (AD), Cisco has produced a whitepaper that provides a detailed explanation of how to perform Cisco Unified Communications Manager integration with AD using the least-privileged principle. The whitepaper can be downloaded here:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a0080a83435.shtml

Additional mitigation techniques that can be deployed on Cisco devices within the network are available in the Cisco Applied Mitigation Bulletin companion document for this advisory:

<http://www.cisco.com/warp/public/707/cisco-amb-20090311-cucmpab.shtml>

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

☐ Obtaining Fixed Software

Cisco has released free software updates that address these vulnerabilities. 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.

The vulnerability in Cisco Unified Communications Manager 4.x software versions was reported to

Cisco by Olivier Grosjeanne of Dimension Data France. The vulnerability in Cisco Unified Communications Manager 5.x, 6.x and 7.x software versions was reported by Oliver Dewdney of LBI.

[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.

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

☐ **Distribution**

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

<http://www.cisco.com/warp/public/707/cisco-sa-20090311-cucmpab.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.

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

☐ Revision History

Revision 1.0	2009-March-11	Initial public release.
--------------	---------------	-------------------------

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

☐ 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 Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

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

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](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 - 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) |

[Trademarks of Cisco Systems, Inc.](#)