

Cisco Security Advisory: Cisco Personal Assistant User Password Bypass Vulnerability

Document ID: 47765

Advisory ID: cisco-sa-20040108-pa

<http://www.cisco.com/warp/public/707/cisco-sa-20040108-pa.shtml>

Revision 1.0

For Public Release 2004 January 8 1700 UTC (GMT)

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

[Summary](#)

[Affected Products](#)

[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 Personal Assistant may permit unauthorized access to user configuration via the web interface. Once access is granted, user preferences and configuration can be manipulated.

There is a workaround available and a software upgrade is not required to remove the vulnerability.

This issue is documented in Cisco Bug ID CSCec87825.

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20040108-pa.shtml>

Affected Products

This section provides details on affected products.

Vulnerable Products

Cisco Personal Assistant versions 1.4(1) and 1.4(2) only are affected. Cisco Personal Assistant versions 1.3(x) and prior are not affected.

To verify the version of Personal Assistant you are running, perform the following steps.

1. Log in to Personal Assistant through the web interface.
2. Browse to **Help** -> **About Cisco Personal Assistant**.
3. Click the **Details** button and a window appears with the full version number.

Products Confirmed Not Vulnerable

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

Details

Cisco Personal Assistant is a Microsoft Windows 2000 based application and is part of the AVVID solution. For more information on Personal Assistant, see:

<http://www.cisco.com/en/US/partner/products/sw/voicesw/ps2026/index.html>

This vulnerability is only present if both of the following conditions are met:

- The Personal Assistant administrator has checked the "Allow Only Cisco CallManager Users" box through **System** -> **Miscellaneous Settings**.
- The Personal Assistant Corporate Directory settings refer to the same directory service that is used by Cisco CallManager.

If both of the above criteria are met, then password authentication to Personal Assistant user configuration is disabled. This allows anyone to enter a valid User ID with any password and the user will be authorized to make configuration changes to that account.

The default setting for Personal Assistant is that the "Allow Only Cisco CallManager Users" box is unchecked.

Users access Personal Assistant by browsing to the address **http://x.x.x.x/pauseradmin** where x.x.x.x is the IP address or hostname of the Personal Assistant server.

This vulnerability does not affect access to Personal Assistant through the telephony interface. Users access the telephony interface by dialing the Personal Assistant extension. Personal Assistant uses the user's CallManager Extension Mobility PIN or the Unity Subscriber Phone Password to authenticate users through the telephony interface.

This vulnerability is documented as Cisco bug ID [CSCec87825](#)

Impact

This bug permits unauthorized configuration access to users' Personal Assistant settings. This vulnerability does not affect the system configuration of the Personal Assistant application.

An attacker can modify the settings of a user, which can include modifying call routing to redirect calls for purposes of impersonation, or forwarding the user's number to a toll number, incurring charges.

Software Versions and Fixes

All vulnerabilities listed in this advisory can be removed through configuration of the Personal Assistant server. No software update is required.

Workarounds

This vulnerability can be removed by de-selecting the checkbox "Allow Only Cisco CallManager Users" on the **System** -> **Miscellaneous Settings** page of the Personal Assistant Administration site.

This workaround will have no effect on the behavior of the Personal Assistant as CallManager and Personal Assistant must be configured to use the same directory for this vulnerability to be present. Configuring "Allow Only CallManager Users" while having Personal Assistant and CallManager using the same directory is technically redundant.

Obtaining Fixed Software

Cisco has made free software available to address this vulnerability for affected customers. 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/public/sw-license-agreement.html>, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact either "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 agreement 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 who do not hold a Cisco service contract and customers who purchase through third-party vendors but are unsuccessful at obtaining fixed software through their point of sale should get their 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

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

Refer to <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> for additional TAC contact information, including special localized telephone numbers and instructions and e-mail addresses for use in various languages.

Exploitation and Public Announcements

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerability described in this advisory.

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 will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20040108-pa.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
- bugtraq@securityfocus.com
- first-teams@first.org (includes CERT/CC)
- cisco@spot.colorado.edu
- comp.dcom.sys.cisco
- firewalls@lists.gnac.com
- Various internal Cisco mailing lists

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	08 January 2004	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 Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).

Updated: Jan 08, 2004

Document ID: 47765
