

# Table of Contents

<b><u>Cisco Security Advisory: Cisco Unity Integrated with Exchange Has Default Passwords</u></b> .....	1
<u>Document ID: 63568</u> .....	1
<u>Revision 1.1</u> .....	1
<u>Last Updated 2004 December 17 1745 UTC (GMT)</u> .....	1
<u>For Public Release 2004 December 15 1600 UTC (GMT)</u> .....	1
<u>Please provide your feedback on this document</u> .....	1
<u>Summary</u> .....	1
<u>Affected Products</u> .....	1
<u>Vulnerable Products</u> .....	1
<u>Products Confirmed Not Vulnerable</u> .....	2
<u>Details</u> .....	2
<u>Impact</u> .....	2
<u>Software Versions and Fixes</u> .....	3
<u>Obtaining Fixed Software</u> .....	3
<u>Workarounds</u> .....	3
<u>Exploitation and Public Announcements</u> .....	4
<u>Status of This Notice: FINAL</u> .....	4
<u>Distribution</u> .....	4
<u>Revision History</u> .....	5
<u>Cisco Security Procedures</u> .....	5

# Cisco Security Advisory: Cisco Unity Integrated with Exchange Has Default Passwords

Document ID: 63568

## Revision 1.1

Last Updated 2004 December 17 1745 UTC (GMT)

For Public Release 2004 December 15 1600 UTC (GMT)

---

Please provide your feedback on this document.

---

**Summary**  
**Affected Products**  
**Details**  
**Impact**  
**Software Versions and Fixes**  
**Obtaining Fixed Software**  
**Workarounds**  
**Exploitation and Public Announcements**  
**Status of This Notice: FINAL**  
**Distribution**  
**Revision History**  
**Cisco Security Procedures**

---

## Summary

Several default username/password combinations are present in all available releases of Cisco Unity when integrated with Microsoft Exchange. The accounts include a privileged administrative account, as well as several messaging accounts used for integration with other systems. An unauthorized user may be able to use these default accounts to read incoming and outgoing messages, and perform administrative functions on the Unity system.

This vulnerability is documented in the Cisco Bug Toolkit as Bug ID CSCeg08552 ( registered customers only)

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20041215-unity.shtml>

## Affected Products

### Vulnerable Products

Cisco Unity versions 2.x, 3.x, and 4.x when integrated with Microsoft Exchange.

## Products Confirmed Not Vulnerable

The following products are confirmed not vulnerable:

- Any version of Cisco Unity when integrated with Lotus Notes
- Cisco Unity Express
- Cisco CallManager and CallManager Express
- Cisco MeetingPlace

No other Cisco products are currently known to create these specific default account/passwords.

## Details

Cisco Unity is a communications solution which delivers unified messaging (e-mail, voice, and fax messages sent to one inbox) and intelligent voice messaging. Cisco Unity integrates with desktop applications such as Microsoft Outlook and Lotus Notes.

Several default username/password combinations are present in all releases Cisco Unity when integrated with Microsoft Exchange.

An unauthorized user may be able to use these default accounts to read incoming and outgoing messages, or to perform administrative functions on the Unity system.

The specified accounts with default passwords are:

- **EAdmin<systemid>**
- **UNITY\_<servername>**
- **UAMIS\_<servername>**
- **UOMNI\_<servername>**
- **UVPIM\_<servername>**
- **ESubscriber**

This vulnerability is documented in the Cisco Bug Toolkit as Bug ID CSCeg08552 ( registered customers only)

## Impact

An unauthorized user may utilize EAdmin<systemid> to access the Cisco Unity Administrator in order to create, edit, or delete classes of service, restriction tables, call routing tables, call handlers, schedules and holidays, subscribers, public distribution lists, or to perform other administrative functions.

An unauthorized user may utilize UNITY\_<servername>, UAMIS\_<servername>, UOMNI\_<servername>, or UVPIM\_<servername> to read incoming and outgoing messages as they are passed to and from external voicemail systems. Please note that local messages which do not pass to non-Unity voicemail systems are not made visible by this vulnerability.

ESubscriber is an example user account that conveys no administrative or other special abilities. However it is contrary to best security practices to have unused accounts with default passwords.

# Software Versions and Fixes

Cisco Unity 4.0(5), which is scheduled for released in the first quarter of the calendar year 2005, will contain the fix for this issue for NEW INSTALLS ONLY.

**Note:** An upgrade to Cisco Unity 4.0(5) from any previous version will still contain this vulnerability. Customers upgrading to version 4.0(5) from any previous version must apply the workaround listed below to eliminate the vulnerability.

## Obtaining Fixed Software

As the fix for this vulnerability is a default configuration change, and a workaround is available, a software upgrade is not required to address this vulnerability. However, if you have a service contract, and wish to upgrade to unaffected code, you may obtain upgraded software through your regular update channels once that software is available. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's Worldwide Web site at <http://www.cisco.com>

If you need assistance with the implementation of the workarounds, or have questions on the workarounds, please contact the Cisco Technical Assistance Center (TAC).

- +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](mailto:tac@cisco.com)

See <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.

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>

## Workarounds

It is recommended to change to a strong password for all accounts created by Cisco Unity.

The accounts that are created automatically when Cisco Unity is integrated with Microsoft Exchange are: (replacing <servername> with that of the particular Unity server, and <systemid> with that of your particular system id)

- **EAdmin<systemid>**
- **Unity\_<servername>**
- **UAMIS\_<servername>**
- **UOMNI\_<servername>**
- **UVPIM\_<servername>**
- **Esubscriber**

**Note:** Please note that the account ESubscriber is only created during installation of versions PRIOR to version 4.0(3). If your initial installation of Unity was 4.0(3) or later, Esubscriber will not be present.

Cisco Security Advisory: Cisco Unity Integrated with Exchange Has Default Passwords

See

[http://www.cisco.com/en/US/customer/products/sw/voicesw/ps2237/products\\_tech\\_note09186a0080093f54.shtml](http://www.cisco.com/en/US/customer/products/sw/voicesw/ps2237/products_tech_note09186a0080093f54.shtml) for additional information on how to change account passwords.

For guidance on strong passwords, please refer to your security policy.

The CERT Coordination Center also has suggestions on strong password policy at [http://www.cert.org/tech\\_tips/unix\\_configuration\\_guidelines.html#A](http://www.cert.org/tech_tips/unix_configuration_guidelines.html#A)

Optionally, a customer may disable (but not delete), these specific accounts for extra security. Beginning with version 4.0(5) of Cisco Unity, these specific accounts will be created in a disabled state. For additional instructions on how to disable these accounts, please see <http://www.microsoft.com/windows2000/en/advanced/help/default.asp?url=/windows2000/en/advanced/help/dsadmin>.

With the exception of Esubscriber, it is important to NOT delete any of the accounts listed above. Deletion of EAdmin<systemid>, Unity\_<servername>, UAMIS\_<servername>, UOMIN\_<server>, or UPVIM\_<servername> will have an adverse affect on Cisco Unity operation.

No interruption of service, nor restart of Cisco Unity is required to apply this workarouund.

## 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 discovered during internal Cisco security review.

## Status of This Notice: FINAL

THIS ADVISORY IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY. YOUR USE OF THE INFORMATION ON THE ADVISORY OR MATERIALS LINKED FROM THE ADVISORY IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS NOTICE AT ANY TIME.

## Distribution

This advisory will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20041215-unity.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](mailto:cust-security-announce@cisco.com)
- [first-teams@first.org](mailto:first-teams@first.org) (includes CERT/CC)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [vulnwatch@vulnwatch.org](mailto:vulnwatch@vulnwatch.org)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [cisco-nsp@puck.nether.net](mailto:cisco-nsp@puck.nether.net)
- [full-disclosure@lists.netsys.com](mailto:full-disclosure@lists.netsys.com)
- [comp.dcom.sys.cisco@newsgate.cisco.com](mailto: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 1.1	<del>2004–December–17</del>	Minor typographical corrections.
Revision 1.0	<del>2004–December–15</del>	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](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 © 1992–2004 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

---

Updated: Dec 17, 2004

Document ID: 63568

---