Cisco Security Advisory: Cisco Unity Express Expired Password Reset Privilege Escalation

Document ID: 70043

Advisory ID: cisco−sa−20060501−cue

http://www.cisco.com/warp/public/707/cisco−sa−20060501−cue.shtml

Revision 1.0

For Public Release 2006 May 01 2300 UTC (GMT)

Please provide your feedback on this document.

Summary

Cisco Unity Express (CUE) contains a vulnerability that might allow an authenticated user to change the password for another user by using the HTTP management interface, if the password for the user being modified is marked as expired. This can result in a privilege escalation attack and complete administrative control of a CUE module, if the password being changed belongs to an administrator.

There are mitigations for this vulnerability.

Cisco has made free software available to address this vulnerability for affected customers.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco−sa−20060501−cue.shtml.

Affected Products

This section provides details on affected products.

Vulnerable Products

Any CUE Advanced Integration Module (AIM) or Network Module (NM) running CUE software versions prior to 2.3(1) is affected by this vulnerability.

The version of software running on a CUE module can be determined using the **show software versions** command in the CUE command line interface or by selecting **Help > About** in the HTTP management interface.

```
cue-10-0-0-1# show software versions
Installed Packages:
 - Bootloader (Primary)  2.1.2
 - Global  2.2.0
 - GPL Infrastructure 2.1.2
 - Voice Mail  2.1.2
 - Bootloader (Secondary)  2.1.2
 - Installer  2.1.1
 - Core  2.1.2
 - Auto Attendant  2.1.2

Installed Languages:
- US English  2.1.0
Installed Languages:
 - US English  1.1.1
```

The CUE version is determined by the Global package.

Products Confirmed Not Vulnerable

No other Cisco products, including Cisco Unity, are currently known to be affected this vulnerability.

Details

Cisco Unity Express (CUE) is an optional hardware module designed for use with Cisco modular routers to provide voice mail and automated attendant services. The HTTP management interface of a CUE module allows authenticated users to change their password. This vulnerability allows authenticated users to change the password for any user with an expired password. If an administrator's account has expired, the administrator's password can be changed allowing an unprivileged user to gain complete administrative control of a CUE module.

There are three ways for a user to have an expired password.

- Newly created users with blank passwords. CUE treats blank passwords as expired. This feature was introduced in CUE software version 1.1(1).
- Newly created users with a randomly selected password. Administrators can elect to have a random password assigned when creating new users. CUE treats the random passwords as expired. This feature was introduced in CUE software version 1.1(1).
- If the system−wide password expiry feature is enabled, user passwords can be configured to expire after a specified number of days. Users with expired passwords are required to change their password. This feature was introduced in CUE software version 2.1(1).

The vulnerability is documented in the following Cisco Bug ID:

- **CSCsd50387 (registered customers only)** Cisco Unity Express Expired Password Reset Privilege Escalation

Impact

Successful exploitation of the vulnerability may allow an unprivileged user to gain complete administrative control of a CUE module. This may result in the disclosure of sensitive information contained in voice mail

stored on a CUE module and possible negative publicity if automated attendant messages are maliciously changed.

Software Version 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.

Fixed software can be downloaded at http://www.cisco.com/cgi−bin/tablebuild.pl/cue−231?psrtdcat20e2.

Affected Releases	First Fixed Release
All CUE releases up to 2.2(2)	2.3(1)

Workarounds

It is possible to mitigate this vulnerability by restricting access to the HTTP management interface to trusted management hosts with an access control list (ACL) applied on the router hosting the CUE module. This will prevent users from accessing some CUE functionality such as setting their display name. Users can continue to access their voice mail and perform a limited number of configuration changes such as updating their personal identification number (PIN). Management functions can be performed using the CUE command line interface.

Obtaining Fixed Software

Cisco has made free software available to address this vulnerability for affected customers. This advisory will be updated as fixed software becomes available. 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.

This vulnerability was reported to Cisco by Xu He and Keith Vaughan of the Bank of America Application Assessment Team.

Status of this Notice: FINAL

Distribution

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

http://www.cisco.com/warp/public/707/cisco−sa−20060501−cue.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−teams@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	2006−May−01	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.

Updated: May 01, 2006 Document ID: 70043