

[NEWS] Cisco Call Manager Privilege Escalation

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-01/msg00074.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 19 Jan 2006 16:49:13 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Cisco Call Manager Privilege Escalation

SUMMARY

Cisco CallManager (CCM) is "the software-based call-processing component of the Cisco IP telephony solution which extends enterprise telephony features and functions to packet telephony network devices such as IP phones, media processing devices, voice-over-IP (VoIP) gateways, and multimedia applications". Cisco CallManager versions with Multi Level Administration (MLA) enabled may be vulnerable to privilege escalations, which may result in read-only users gaining administrative access.

Successful exploitation of the vulnerability may result in privilege escalation where read-only administrative users can gain full administrative privileges and create, delete, or reset devices.

DETAILS

Vulnerable Systems:

- * Cisco CallManager 3.2 and earlier
- * Cisco CallManager 3.3, versions earlier than 3.3(5)SR1
- * Cisco CallManager 4.0, versions earlier than 4.0(2a)SR2c
- * Cisco CallManager 4.1, versions earlier than 4.1(3)SR2

[NEWS] Cisco Call Manager Privilege Escalation

Complete this procedure to check if Multi Level Administration is enabled:

1. Access CCM Administration with this URL: <http://<CCMServer>/ccmadmin>, where <CCMServer> specifies the IP address or name of the Cisco CallManager server.
2. Choose User > Access Rights > Configure MLA Parameters. The MLA Enterprise Parameter Configuration page displays.
3. MLA is enabled if the Enable MultiLevelAdmin enterprise parameter is set to True.

An administrative user with read-only permission can use a crafted URL on the CCMAdmin web page to escalate privileges to a full administrative level. This vulnerability applies to users who are authenticated to the read-only administrative level. Users with no administrative access and users with full administrative permissions continue to work as expected.

Administrative users with access privilege Read Only should not be confused with the standard User Group named "Read Only" which is created at installation. For further details on user groups and assigning access privileges, please refer to this URL:

[http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_administration_guide_chapter09186a00803ed6ea](http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_administration_guide_chapter09186a00803ed6ea.html)
Multilevel Administration Access Configuration

* CSCef75361, CSCsb12765, CSCsb88649, CSCsc26275?CCMAdmin Read Only User Can Escalate Privileges

It is possible to eliminate the ability for an attacker to escalate privileges from Read Only to Full Access without applying the service release by not using the Read Only access privilege, but instead only using the No Access or Full Access privileges. This is not an ideal solution, but can provide a temporary workaround.

For detailed instructions on configuring the privileges for a User Group within Cisco CallManager 4.1(3) see the Multilevel Administration Access Configuration:

[http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_administration_guide_chapter09186a00803ed6ea](http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_administration_guide_chapter09186a00803ed6ea.html)
Assigning Privileges to a User Group

Section of the Cisco CallManager Administration Guide:

[http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_administration_guide_book09186a00803be4ec.ht](http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_administration_guide_book09186a00803be4ec.html)
Cisco CallManager Administration Guide, Release 4.1(3)

ADDITIONAL INFORMATION

The original article can be found at:

<http://www.cisco.com/warp/public/707/cisco-sa-20060118-ccmpe.shtml>
<http://www.cisco.com/warp/public/707/cisco-sa-20060118-ccmpe.shtml>

[NEWS] Cisco Call Manager Privilege Escalation

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

- Prev by Date: [*\[NEWS\] Cisco Call Manager DoS*](#)
- Next by Date: [*\[NEWS\] Blogger.com HTTP Response Splitting Vulnerability*](#)
- Previous by thread: [*\[NEWS\] Cisco Call Manager DoS*](#)
- Next by thread: [*\[NEWS\] Blogger.com HTTP Response Splitting Vulnerability*](#)
- Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)