

Cisco Security Response: SIP User Directory Information Disclosure

Document ID: 70852

<http://www.cisco.com/warp/public/707/cisco-sr-20060802-sip.shtml>

Revision 1.0

For Public Release 2006 August 02 1600 UTC (GMT)

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

[Cisco Response](#)
[Additional Information](#)
[Revision History](#)
[Cisco Security Procedures](#)

Cisco Response

This is the Cisco PSIRT response to the statements made by Dave Endler and Mark Collier in their presentation, 'Hacking Voice over IP (VoIP) Exposed' at BlackHat USA 2006.

We would like to thank Dave Endler for reporting this issue to us.

We greatly appreciate the opportunity to work with researchers on security vulnerabilities, and welcome the opportunity to review and assist in product reports.

This issue is currently being tracked by Cisco bug ID [CSCse92417](#) ([registered](#) customers only) for IOS CallManager Express (CME).

Cisco CallManager has been tested and is not vulnerable to this attack.

Additional Information

The attacks described in the report attempt to manipulate the Session Initiation Protocol (SIP) stack in various voice products to gain information from the SIP user directory. By sending various SIP messages to the VoIP infrastructure, an attacker can discover the names of the users stored in the SIP user database.

It is important to note that the attacks described do not disrupt VoIP call processing or voice mail access.

Cisco's recommended best practice of implementing the VoIP infrastructure and data devices on separate VLANs would prevent malicious users from launching such attacks against the VoIP network.

Please consult the following links for other recommendations and guidelines for securing IP telephony networks:

- Enhanced Security for Unified Communications
http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_package.html

- Cisco Unified Voice Security
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/5x/50scurty.html

Cisco was made aware of this issue on July 20, 2006. We are continuing to investigate this issue and will update this document as additional information becomes available.

Revision History

Revision 1.0	2006 August 02	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>.

[Contacts & Feedback](#) | [Help](#) | [Site Map](#) © 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Aug 02, 2006

Document ID: 70852
