Cisco Security Advisory

Cisco Unified Communications Manager Device Registration SQL Injection Vulnerability

Medium

Advisory ID: Cisco-SA-20120229-CVE-2011-4487
Published: 2012 February 29 16:23 GMT
Version1.0: Final
CVSS Score: Base - 5.8
Workarounds: See below
Cisco Bug IDs: CSCtu73538

CVE-2011-4487
CWE-94

Download CVRF
Download PDF
Email

Summary

Cisco Unified Communications Manager contains a vulnerability that could allow an unauthenticated, remote attacker to execute arbitrary commands in a database underlying the affected application.

The vulnerability is due to improper sanitization of input in device registration requests. An unauthenticated, remote attacker could exploit this vulnerability by sending malicious requests to the targeted system. If successful, the attacker could modify application database contents.

Cisco has confirmed the vulnerability in a security advisory and released software updates.

To exploit the vulnerability, an attacker must be able to send device registration requests over the network to the targeted system. This action would likely require that an attacker have internal network access to conduct an exploit. Most sites restrict external access to affected systems The access requirement reduces the potential for attack.

Cisco indicates through the CVSS score that functional exploit code exists; however, the code is not known to be publicly available.

Affected Products

Cisco has released a security advisory for Cisco bug ID CSCtu73538 at the following link: cisco-sa-20120229-cucm

Vulnerable Products

The following Cisco products are affected:

- Cisco Unified Communications Manager versions prior to 8.0(3a)su3
- Cisco Unified Communications Manager versions prior to 8.6(2a)su1
- Cisco Business Edition 3000 Software versions prior to 8.6.3
- Cisco Business Edition 5000 Software versions prior to 8.6(2a)su1
- Cisco Business Edition 6000 Software versions prior to 8.6(2a)su1

Products Confirmed Not Vulnerable

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

Workarounds

Administrators are advised to apply the appropriate updates.

Administrators may consider using IP-based access control lists (ACLs) to allow only trusted systems to access the affected systems.

Administrators are advised to monitor affected systems.

The Cisco Applied Intelligence team has created the following companion document to guide administrators in identifying and mitigating attempts to exploit this vulnerability prior to applying updated software: cisco-amb-20120229-cucm

Fixed Software

Cisco customers with active contracts can obtain updates through the Software Center at the following link: Cisco. Cisco customers without contracts can obtain upgrades by contacting the Cisco Technical Assistance Center at 1-800-553-2447 or 1-408-526-7209 or via e-mail at tac@cisco.com.

Exploitation and Public Announcements

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20120229-CVE-2011-4487

Revision History

Version	Description	Section	Status	Date
1.0	Initial Release	NA	Final	2012-Feb-29

Legal Disclaimer

Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the Security Vulnerability Policy. This document also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

Related Resources

SA Cisco Unified Communications Manager Skinny Client Control Protocol Vulnerabilities

Subscribe to Cisco Security Notifications

Subscribe