Cisco Security Advisory

Cisco Unified Communications Manager Potential SQL Injection Vulnerability

Advisory ID: Cisco-SA-20110427-CVE-2011-1610
Last Updated: 2012 July 14 13:02 GMT
Published: 2011 April 27 15:10 GMT
Version2.0: Final
CVSS Score: Base - 6.4
Workarounds: See below

CVE-2011-1610
CWE-264

Download CVRF
Download PDF
Email

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

ST 21377

IPS Cisco Call Manager SQL Injection

Subscribe to Cisco Security Notifications

Subscribe

Summary

Cisco Unified Communications Manager contains a vulnerability that could allow an unauthenticated, remote attacker to conduct SQL injection on a vulnerable system.

The vulnerability is in a JavaServer Pages (JSP) script due to insufficient checks on user-supplied input. An unauthenticated, remote attacker could exploit this vulnerability by submitting crafted parameters that contain malicious SQL commands to the vulnerable script. The processing of these parameters could allow the attacker to execute arbitrary SQL commands that could lead to a modification of sensitive information in the underlying database.

Cisco has confirmed this vulnerability and has released updated software.

To exploit the vulnerability, an attacker would need to be able to access the Cisco Unified Communications Manager and inject SQL commands on the vulnerable system. Depending on network configurations, an attacker may need access to internal networks. The access requirement could increase the difficulty of an exploit.

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 CSCtj42064 at the following link: cisco-sa-20110427-cucm

Vulnerable Products

Cisco Unified Communications Manager versions prior to 6.1(5)su2, 7.1(5)su4 , 8.0(3a)su2, and 8.5(1)su1 are vulnerable.

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 implement an intrusion prevention system (IPS) or intrusion detection system (IDS) to help detect and prevent attacks that attempt to exploit this vulnerability.

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-20110427-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-20110427-CVE-2011-1610

Revision History

Version	Description	Section	Status	Date
1.0	Initial Release	NA	Final	2011-Apr-27

Legal Disclaimer