Cisco Security Advisory

Cisco IOS Software and Cisco Unified Communications Manager Session Initiation Protocol Packet Processing Memory Leak Vulnerability

Advisory ID: Cisco-SA-20111107-CVE-2011-0941
Published: 2011 November 7 16:36 GMT
Version1.0: Final
CVSS Score: Base - 7.8
Workarounds: See below
Cisco Bug IDs: CSCtj09179

CVE-2011-0941
CWE-399

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.

Subscribe to Cisco Security Notifications

Subscribe

Summary

Cisco IOS Software and Cisco Unified Communications Manager contain a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

The vulnerability is due to improper processing of malformed packets by the affected software. An unauthenticated, remote attacker could exploit this vulnerability by sending malicious network requests to the targeted system. If successful, the attacker could cause the device to become unresponsive, resulting in a DoS condition.

Cisco confirmed this vulnerability and released software updates.

To exploit the vulnerability, an attacker must send malicious SIP packets to affected systems. Most environments restrict external connections using SIP, likely requiring an attacker to have access to internal networks prior to an attack. In addition, in environments that separate voice and data networks, attackers may have no access to networks that service voice traffic and allow the transmission of SIP packets, further increasing 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 issued release notes in the following bug IDs: CSCti75128 and CSCtj09179

Vulnerable Products

Cisco Unified Communications Manager versions prior to 8.5(1), 8.0(3a)su1, 7.1(5b)su3, and 6.1(5)su2 are vulnerable. Cisco has published a list of affected Cisco IOS Software releases in Cisco bug ID CSCtj09179. The Vendor Announcements section of this alert contains a link to the bug ID.

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 may consider disabling SIP processing on devices that do not require it.

Administrators are advised to monitor affected systems.

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-20111107-CVE-2011-0941

Revision History

Version	Description	Section	Status	Date
1.0	Initial Release	NA	Final	2011-Nov-07

Legal Disclaimer