Cisco Security Advisory

Cisco Unified Communications Manager Multiple Denial of Service Vulnerabilities

Advisory ID: cisco-sa-20130227-cucm
Published: 2013 February 27 16:00 GMT
Version1.0: Final
CVSS Score: Base - 7.8
Workarounds: See below
Cisco Bug IDs: CSCtx43337 CSCub28920

CVE-2013-1133
CVE-2013-1134
CWE-20
CWE-264

Download CVRF
Download PDF
Email

Summary

Cisco Unified Communications Manager contains two vulnerabilities that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. Exploitation of these vulnerabilities could cause an interruption of voice services.

Cisco has released software updates that address these vulnerabilities. This advisory is available at the following link: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130227-cucm

Affected Products

Vulnerable Products

The following products are affected by the vulnerabilities that are described in this advisory:

- Cisco Unified Communications Manager 8.6(x)
- Cisco Unified Communications Manager 9.0(x)

Note: Cisco Unified Communications Manager version 6.1 reached the End of Software Maintenance on September 3, 2011. Customers using Cisco Unified Communications Manager 6.x versions should contact their Cisco support team for assistance in upgrading to a supported version of Cisco Unified Communications Manager.

Products Confirmed Not Vulnerable

The following products are not affected by the vulnerabilities described in this advisory.

- Cisco Unified Communications Manager 7.x
- Cisco Unified Communications Manager 8.5(x)

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

Details

Cisco Unified Communications Manager is the call processing component of the Cisco IP Telephony solution that extends enterprise telephony features and functions to packet telephony network devices, such as IP phones, media processing devices, VoIP gateways, and multimedia applications.

Malformed UDP Packets Denial of Service Vulnerability

Cisco Unified Communications Manager contains a DoS vulnerability that could allow an unauthenticated, remote attacker to cause an exhaustion of resources in the CPU. This vulnerability is triggered by receiving malformed packets on unused UDP ports and could result in an inability to connect to the graphical user interface (GUI) and an interruption of voice services.

This vulnerability is documented in Cisco Bug ID CSCtx43337 (registered customers only) and has been assigned the Common Vulnerabilities Enumerator (CVE) ID CVE-2013-1133. This vulnerability applies to Cisco Unified Communications Manager versions 8.6(x) and above and is fixed in Cisco Unified Communications Manager versions 9.0(1), 8.6(4) BE3k and 8.6(2a)su2. Cisco Unified Communications Manager 7.1(x) and 8.5(x) versions are not affected.

Location Bandwidth Manager (LBM) Cache Poisoning Vulnerability

Cisco Unified Communications Manager 9.0 contains a vulnerability that could allow an unauthenticated, remote attacker to poison the Location Bandwidth Manager (LBM) transaction records.

The vulnerability is due to a lack of authentication of the remote LBM Hub node in the Intracluster communication between LBMs. An attacker could exploit this vulnerability by poisoning the LBM transaction records to consume all available bandwidth pools. An exploit could allow the attacker to consume all bandwidth and deny calls. This vulnerability is documented in Cisco Bug ID CSCub28920 (registered customers only) and has been assigned the CVE ID CVE-2013-1134. This vulnerability applies to Cisco Unified Communications Manager version 9.0(x) only and is fixed in Cisco Unified Communications Manager versions 9.1(1). Cisco Unified Communications Manager 7.1(x), 8.5(x) and 8.6(x) versions are not affected.

Workarounds

Filtering traffic on TCP port 9004 from untrusted sources can provide a workaround for the LBM vulnerability.

Additional mitigations that can be deployed on Cisco devices in the network are available in the companion document "Identifying and Mitigating Exploitation of the Cisco Unified Communications Manager and Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerability" at the following location: http://tools.cisco.com/security/center/viewAMBAlert.x?alertId=28034

Fixed Software

When considering software upgrades, also consult http://www.cisco.com/go/psirt and any subsequent advisories to determine exposure and a complete upgrade solution. Cisco recommends upgrading to a release equal to or later than the release in the "Recommended Release" column of the table.

Cisco Unified Communication Manager Version	Recommended Release
8.x	8.6(4)BE3K, 8.6(2a)su2
9.x	9.1(1)

In all cases, customers should ensure that the devices to be upgraded contain sufficient memory and confirm that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, customers are advised to contact the Cisco Technical Assistance Center (TAC) or their contracted maintenance providers.

Exploitation and Public Announcements

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

These vulnerabilities were found during internal testing.

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130227-cucm

---

Revision History

Revision 1.0	2013-February-27	Initial public release.

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

IS Cisco Unified Communications Manager UDP Closed Ports Denial of Service Vulnerability

IS Cisco Unified Communications Manager Location Bandwidth Manager Poisoning Vulnerability

AMB Identification and Mitigation of Vulnerabilities in Cisco Voice and Unified Communications Products

Subscribe to Cisco Security Notifications

Subscribe