Cisco Security Advisory

Multiple Vulnerabilities in Cisco Unified Communications Manager

High

Advisory ID: cisco-sa-20130821-cucm
Published: 2013 August 21 16:00 GMT
Version1.0: Final
CVSS Score: Base - 8.5
Workarounds: See below
Cisco Bug IDs: CSCub35869 CSCub85597 CSCud54358 CSCuf93466

CVE-2013-3459
CVE-2013-3460
CVE-2013-3461
CVE-2013-3462
CWE-119
CWE-20
CWE

Download CVRF
Download PDF
Email

Summary

Cisco Unified Communications Manager (Unified CM) contains multiple vulnerabilities that could allow an unauthenticated, remote attacker to modify data, execute arbitrary commands, or cause a denial of service (DoS) condition.

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-20130821-cucm

Affected Products

Vulnerable Products

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

- Cisco Unified Communications Manager 7.1(x)
- Cisco Unified Communications Manager 8.5(x)
- Cisco Unified Communications Manager 8.6(x)
- Cisco Unified Communications Manager 9.0(x)
- Cisco Unified Communications Manager 9.1(x)

Note: Cisco Unified Communications Manager version 8.0 reached the End of Software Maintenance on October 23, 2012. Customers using Cisco Unified Communications Manager 8.0(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

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. Cisco Unified Communications Manager contains multiple vulnerabilities that could allow an unauthenticated, remote attacker to cause a DoS condition or execute code remotely.

Denial of Service Vulnerabilities

Cisco Unified Communications Manager 7.1(x) contains a vulnerability that could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. The vulnerability is due to improper error handling . An attacker could exploit this vulnerability by sending malformed registration messages, resulting in a DoS condition on an affected device. This vulnerability is documented in Cisco bug ID CSCuf93466 (registered customers only) and has been assigned the Common Vulnerabilities and Exposures (CVE) ID CVE-2013-3459. This vulnerability affects only Cisco UCM versions 7.1(x).

Cisco Unified Communications Manager 8.5(x), 8.6(x), and 9.0(x) contain a vulnerability that could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. The vulnerability is due to insufficient limiting of traffic on certain UDP ports. An attacker could exploit this vulnerability by sending UDP packets at a high rate to certain ports on an affected device, resulting in a DoS condition on the affected device. This vulnerability is documented in Cisco bug ID CSCub85597 (registered customers only) and has been assigned the CVE ID CVE-2013-3460.

Cisco Unified Communications Manager versions 8.5(x), 8.6(x) and 9.0(1) contain a vulnerability that could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. The vulnerability is due to insufficient rate limiting of traffic on the Session Initiation Protocol (SIP) port. An attacker could exploit this vulnerability by sending UDP packets at a high rate to port 5060 on an affected device. A sustained attack could allow the attacker to cause a DoS condition on the affected device. This vulnerability is documented in Cisco bug ID CSCub35869 (registered customers only) and has been assigned the Common Vulnerabilities and Exposures CVE ID CVE-2013-3461.

Buffer Overflow Vulnerability

Cisco Unified Communications Manager 7.1(x), 8.5(x), 8.6(x), 9.0(x) and 9.1(x) contain a vulnerability that could allow an authenticated, remote attacker to cause a buffer overflow on an affected device. The vulnerability is due to insufficient bounds checking. An attacker could exploit this vulnerability by overwriting an allocated memory buffer on an affected device. An exploit could allow the attacker to corrupt data, disrupt services, or run arbitrary commands. This vulnerability is documented in Cisco bug ID CSCud54358 (registered customers only) and has been assigned the CVE ID CVE-2013-3462. This vulnerability affects Cisco UCM versions 7.1(x) through 9.1(1x).

Workarounds

No workarounds are available for these vulnerabilities.

Fixed Software

When considering software upgrades, customers are advised to consult the Cisco Security Advisories, Responses, and Notices archive at http://www.cisco.com/go/psirt and review 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 following table:

Identifier	CVE ID	Cisco Unified Communication Manager Version	First Fixed	Recommended Release
CSCud54358: Insufficient Boundary Check of Input Buffer	CVE-2013-3462	7.x	7.1(5b)su6	7.1(5b)su6a
CSCuf93466: Improper Error Handling of Malformed Registration Messages	CVE-2013-3459	7.x	7.1(5b)su6a	7.1(5b)su6a
CSCub85597: Memory Leak Observed During UDP Flood	CVE-2013-3460	8.x	8.5(1)su6, 8.6(2a)su3, 8.6(5)BE3K	8.5(1)su6, 8.6(2a)su3, 8.6(5)BE3K
CSCub35869: High CPU Utilization and Memory Leak During UDP Flood	CVE-2013-3461	8.x	8.6(2a)su3, 8.6(5)BE3K	8.6(2a)su3, 8.6(5)BE3K
CSCud54358: Insufficient Boundary Check of Input Buffer	CVE-2013-3462	8.x	8.5(1)su6, 8.6(2a)su3	8.5(1)su6, 8.6(2a)su3
CSCub85597: Memory Leak Observed During UDP Flood	CVE-2013-3460	9.x	9.1(1)	9.1(2) or later
CSCub35869: High CPU				

Utilization and Memory Leak During UDP Flood	CVE-2013-3461	9.x	9.1(1)	9.1(2) or later
CSCud54358: Insufficient Boundary Check of Input Buffer	CVE-2013-3462	9.x	9.1(2)	9.1(2) or later

***Note:** Cisco Unified Communications Manager Version 8.5(1)su6 is targeted for release in mid-September 2013. Customers running Cisco Unified Communications Manager Version 8.5 are encouraged to upgrade to 8.6 for complete coverage for all vulnerabilities listed in this advisory.

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-20130821-cucm

---

Revision History

Revision 1.0	2013-August-21	Initial public release

Legal Disclaimer