Cisco Security Advisory

# Cisco Unified Communications Manager Remote Blind SQL Injection Vulnerability

Medium

**Advisory ID:** Cisco-SA-20130717-CVE-2013-3404
**Published:** 2013 July 17 16:07 GMT
**Version1.0:** Final
**CVSS Score:** Base - 6.4
**Workarounds:** See below
**Cisco Bug IDs:** CSCuh01051

CVE-2013-3404
CWE-89

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**

SA Multiple Vulnerabilities in Cisco Unified Communications Manager

**Subscribe to Cisco Security Notifications**

Subscribe


## Summary

Cisco Unified Communication Manager (Unified CM) contains a vulnerability that could allow an unauthenticated, remote attacker to execute a blind Structured Query Language (SQL) injection.

The vulnerability is due to improper validation of user-supplied requests by the Cisco Unified CM. An attacker could exploit this vulnerability by injecting SQL commands. An exploit could allow the attacker to leverage metadata to recreate encrypted information within the database. This metadata could be used to reconstruct encrypted credentials.

Proof-of-concept code that demonstrates an exploit of this vulnerability is publicly available.

Cisco has confirmed the vulnerability in a security advisory and has released a temporary fix.

To exploit this vulnerability, an attacker may require access to trusted, internal networks to send crafted requests to the affected software. This access requirement could limit the likelihood of a successful exploit.

Cisco Unified CM version 8.0 reached the End of Software Maintenance on October 23, 2012. Customers using Cisco Unified CM 8.0(x) versions should contact their Cisco support team for assistance in upgrading to a supported version of Cisco Unified CM.

Cisco Unified CM is the only product confirmed to be vulnerable. Additional voice products may be affected by one or more of the individual vulnerabilities that are described in the advisory. The following products are being investigated but have not yet been confirmed as vulnerable:

- Cisco Emergency Responder
- Cisco Unified Contact Center Express
- Cisco Unified Customer Voice Portal
- Cisco Unified Presence Server/Cisco IM and Presence Service
- Cisco Unity Connection

This vulnerability can be exploited over the default management ports, TCP port 8080 or 8443.


## Affected Products

Cisco has released a security advisory for bug ID CSCuh01051 at the following link: cisco-sa-20130717-cucm

### Vulnerable Products

Cisco Unified CM versions 9.1(1a) and prior are affected.

### 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 are advised to contact the vendor regarding future updates and releases.

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: Identifying and Mitigating Exploitation of the Multiple Vulnerabilities in Cisco Unified Communications Manager

For additional information about SQL injection attacks and defenses, see Understanding SQL Injection.

Administrators are advised to allow only trusted users to have network access.

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.

## Fixed Software

Cisco customers with active contracts can obtain updates through the Software Center. 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 email at *tac@cisco.com*.

A Cisco Options Package (COP) file**, cmterm-CSCuh01051-2.cop.sgn**, has been released to the software downloads page in the Utilities section for the affected software. The COP file for 9.1(x) versions would be located by navigating the following path on the software downloads page:

Products Voice and Unified Communications IP Telephony Unified Communications Platform Cisco Unified Communications manager Cisco Unified Communications Manager Version 9.1 Unified Communications Manager/CallManager/Cisco Unity Connection Utilities-COP-Files

## 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-20130717-CVE-2013-3404

---

## Revision History

| Version | Description | Section | Status | Date |
|---|---|---|---|---|
| 1.0 | Initial Release | NA | Final | 2013-Jul-17 |

---