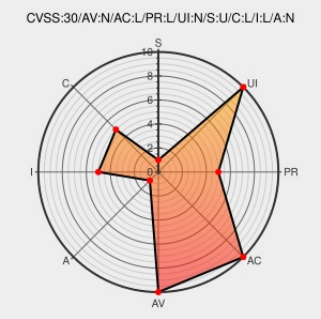
CVE-2019-15972

Published on: 11/25/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:45 PM UTC

CVE-2019-15972 - advisory for cisco-sa-20191120-cucm-sql

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Unified Communications Manager from Cisco contain the following vulnerability:

A vulnerability in the web-based management interface of Cisco Unified Communications Manager could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. The vulnerability exists because the web-based management interface improperly validates SQL values. An attacker could exploit this vulnerability by authenticating to the application and sending malicious requests to an affected system. A successful exploit could allow the attacker to modify values on or return values from the underlying database.

CVE-2019-15972 has been assigned by psirt@cisco.com to track the vulnerability - currently rated as HIGH severity.

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.

Affected Vendor/Software: **Cisco** - **Cisco Unified Communications Manager** version **n/a**

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**

PARTIAL | PARTIAL | PARTIAL

CVE References

Description	Tags	Link
Cisco Unified Communications Manager SQL Injection Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20191120 Cisco Unified Communications Manager SQL Injection Vulnerability

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

Scripts that can be used to exploit CVE-2019-15972 which was an Authenticated SQLi issue in Cisco Unified Call Manage…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Unified Communications Manager	10.5(2.10000.5)	All	All	All
Application	Cisco	Unified Communications Manager	10.5\(2.10000.5\)	All	All	All
Application	Cisco	Unified Communications Manager	11.5(1.10000.6)	All	All	All
Application	Cisco	Unified Communications Manager	11.5\(1.10000.6\)	All	All	All
Application	Cisco	Unified Communications Manager	12.0(1.10000.10)	All	All	All
Application	Cisco	Unified Communications Manager	12.0\(1.10000.10\)	All	All	All
Application	Cisco	Unified Communications Manager	12.5(1.10000.22)	All	All	All
Application	Cisco	Unified Communications Manager	12.5\(1.10000.22\)	All	All	All
Application	Cisco	Unified Communications Manager	10.5\(2.10000.5\)	All	All	All
Application	Cisco	Unified Communications Manager	11.5\(1.10000.6\)	All	All	All
Application	Cisco	Unified Communications Manager	12.0\(1.10000.10\)	All	All	All
Application	Cisco	Unified Communications Manager	12.5\(1.10000.22\)	All	All	All

cpe:2.3:a:cisco:unified_communications_manager:10.5(2.10000.5):*:*:*:*:*:*:*:

cpe:2.3:a:cisco:unified_communications_manager:10.5\(2.10000.5\):*:*:*:*:*:*:*:

cpe:2.3:a:cisco:unified_communications_manager:11.5(1.10000.6):*:*:*:*:*:*:*:

cpe:2.3:a:cisco:unified_communications_manager:11.5\(1.10000.6\):*:*:*:*:*:*:*:

cpe:2.3:a:cisco:unified_communications_manager:12.0(1.10000.10):*:*:*:*:*:*:*:

cpe:2.3:a:cisco:unified_communications_manager:12.0\(1.10000.10\):*:*:*:*:*:*:*:

cpe:2.3:a:cisco:unified_communications_manager:12.5(1.10000.22):*:*:*:*:*:*:*:

cpe:2.3:a:cisco:unified_communications_manager:12.5\(1.10000.22\):*:*:*:*:*:*:*:

cpe:2.3:a:cisco:unified_communications_manager:10.5\(2.10000.5\):*:*:*:*:*:*:*:

cpe:2.3:a:cisco:unified_communications_manager:11.5\(1.10000.6\):*:*:*:*:*:*:*:

cpe:2.3:a:cisco:unified_communications_manager:12.0\(1.10000.10\):*:*:*:*:*:*:*:

cpe:2.3:a:cisco:unified_communications_manager:12.5\(1.10000.22\):*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→