



CVE-2019-19607

Published on: 03/02/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:53 PM UTC

CVE-2019-19607

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Micollab Audio Web Video Conferencing](#) from [Mitel](#) contain the following vulnerability:

A SQL injection vulnerability in the web conferencing component of Mitel MiCollab AWW before 8.1.2.2 could allow an unauthenticated attack due to insufficient input validation for the session parameter. A successful exploit could allow an attacker to extract sensitive information from the database and execute arbitrary scripts.

CVE-2019-19607 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Security Advisories	Vendor Advisory www.mitel.com text/html	MISC www.mitel.com/support/security-advisories

