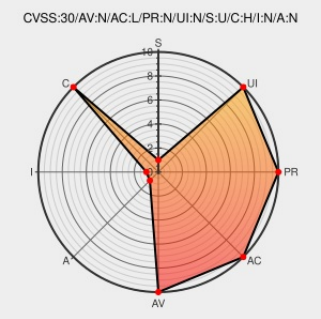
CVE-2016-2164

Published on: 04/11/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:14 PM UTC

CVE-2016-2164

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



Certain versions of Openmeetings from Apache contain the following vulnerability:

The (1) FileService.importFileByInternalUserId and (2) FileService.importFile SOAP API methods in Apache OpenMeetings before 3.1.1 improperly use the Java URL class without checking the specified protocol handler, which allows remote attackers to read arbitrary files by attempting to upload a file.

CVE-2016-2164 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Apache OpenMeetings 3.0.7 Arbitary File Read ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/136434/Apache-OpenMeetings-3.0.7-Arbitary-File-Read.html
Apache OpenMeetings Project – Security	Patch	CONFIRM openmeetings.apache.org/security.html

Apache Openmeetings Project - Security Vulnerabilities	Patch Vendor Advisory openmeetings.apache.org text/html	CONFIRM openmeetings.apache.org/security.html
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20160325 [CVE-2016-2164] Arbitrary file read via SOAP API
404 Not Found	www.apache.org text/plain Inactive Link Not Archived	CONFIRM www.apache.org/dist/openmeetings/3.1.1/CHANGELOG

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Openmeetings	All	All	All	All

cpe:2.3:a:apache:openmeetings:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→