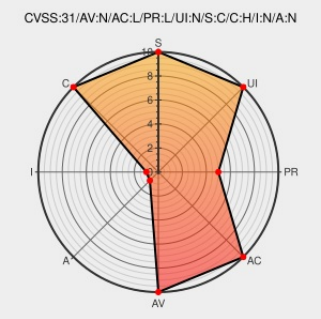
CVE-2021-41152

Published on: 10/18/2021 12:00:00 AM UTC

Last Modified on: 10/22/2021 01:52:00 PM UTC

CVE-2021-41152 - advisory for GHSA-m8j5-837g-2p3f

Source: Mitre | Source: Nist | Print: PDF



Certain versions of Openolat from Frentix contain the following vulnerability:

OpenOlat is a web-based e-learning platform for teaching, learning, assessment and communication, an LMS, a learning management system. In affected versions by manipulating the HTTP request an attacker can modify the path of a requested file download in the folder component to point to anywhere on the target system. The attack could be used to read any file accessible in the web root folder or outside, depending on the configuration of the system and the properly configured permission of the application server user. The attack requires an OpenOlat user account or the enabled guest user feature together with the usage of the folder component in a course. The attack does not allow writing of arbitrary files, it allows only reading of files and also only ready of files that the attacker knows the exact path which is very unlikely at least for OpenOlat data files. The problem is fixed in version 15.5.8 and 16.0.1 It is advised to upgrade to version 16.0.x. There are no known workarounds to fix this problem, an upgrade is necessary.

CVE-2021-41152 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **OpenOLAT** - **OpenOLAT** version **< 15.5.8**

CVSS3 Score: 7.7 - HIGH

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

CVSS2 Score: 4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE

Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Path Traversal in Folder Component Leading to Local File Inclusion · Advisory · OpenOLAT/OpenOLAT · GitHub	github.com text/html	CONFIRM github.com/OpenOLAT/OpenOLAT/security/advisories/GHSA-m8j5-837 2p3f
Log in - OpenOlat Issue Management	jira.openolat.org text/html	MISC jira.openolat.org/browse/OO-5696
OO-5696: validate file selections against current container · OpenOLAT/OpenOLAT@418bb50 · GitHub	github.com text/html	MISC github.com/OpenOLAT/OpenOLAT/commit/418bb509ffcb0e25ab4390563c6c47f0458

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Frentix	Openolat	All	All	All	All

cpe:2.3:a:frentix:openolat:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-41152 : OpenOlat is a web-based e-learning platform for teaching, learning, assessment and communication,… twitter.com/i/web/status/1…	2021-10-18 21:01:30
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2021-41152 Description: OpenOlat is a web-based e-learning platform for teac… twitter.com/i/web/status/1…	2021-10-18 22:00:10

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report