



# CVE-2021-41152

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

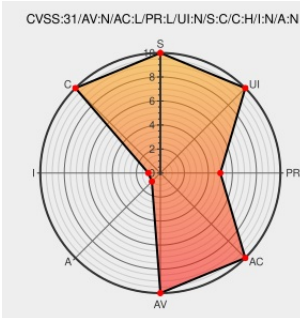
Last Modified on: 10/22/2021 01:52:00 PM UTC

## 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
<b>NETWORK</b>	<b>LOW</b>	<b>LOW</b>	<b>NONE</b>
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
<b>CHANGED</b>	<b>HIGH</b>	<b>NONE</b>	<b>NONE</b>

CVSS2 Score: **4 - MEDIUM**

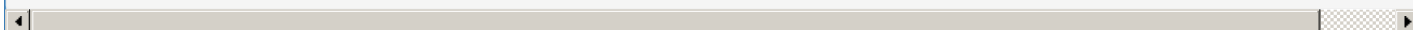
Access Vector	Access Complexity	Authentication
<b>NETWORK</b>	<b>LOW</b>	<b>SINGLE</b>

<b>CONFIDENTIALITY</b>	<b>LOW</b>	<b>SINGLE</b>
<b>Confidentiality Impact</b>	<b>Integrity Impact</b>	<b>Availability Impact</b>
<b>PARTIAL</b>	<b>NONE</b>	<b>NONE</b>

### CVE References

Description	Tags	Link
Path Traversal in Folder Component Leading to Local File Inclusion · Advisory · OpenOLAT/OpenOLAT · GitHub	<a href="#">github.com</a> <a href="#">text/html</a>	CONFIRM <a href="https://github.com/OpenOLAT/OpenOLAT/security/advisories/GHSA-m8j5-8372p3f">github.com/OpenOLAT/OpenOLAT/security/advisories/GHSA-m8j5-8372p3f</a>
Log in - OpenOlat Issue Management	<a href="#">jira.openolat.org</a> <a href="#">text/html</a>	<input type="checkbox"/> MISC <a href="https://jira.openolat.org/browse/OO-5696">jira.openolat.org/browse/OO-5696</a>
OO-5696: validate file selections against current container · OpenOLAT/OpenOLAT@418bb50 · GitHub	<a href="#">github.com</a> <a href="#">text/html</a>	MISC <a href="https://github.com/OpenOLAT/OpenOLAT/commit/418bb509ffc0e25ab4390563c6c47f0458f">github.com/OpenOLAT/OpenOLAT/commit/418bb509ffc0e25ab4390563c6c47f0458f</a>

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](mailto:comment@cve.report).



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
<pre>cpe:2.3:a:frexit:openolat:*:*:*:*:*:*</pre>						

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,... <a href="https://twitter.com/i/web/status/1451152115211521152">twitter.com/i/web/status/1...</a>	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... <a href="https://twitter.com/i/web/status/1451152115211521152">twitter.com/i/web/status/1...</a>	2021-10-18 22:00:10

[← Previous ID](#)

[Next ID →](#)

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**