



# CVE-2021-41132

Published on: 10/14/2021 12:00:00 AM UTC

Last Modified on: 10/20/2021 07:14:00 PM UTC

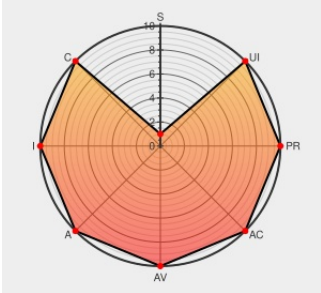
## CVE-2021-41132 - advisory for GHSA-g67g-hvc3-xmvf

[Source: Mitre](#)

[Source: Nist](#)

[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Omero-figure](#) from [Openmicroscopy](#) contain the following vulnerability:

OMERO.web provides a web based client and plugin infrastructure. In versions prior to 5.11.0, a variety of templates do not perform proper sanitization through HTML escaping. Due to the lack of sanitization and use of ``jQuery.html()`, there are a whole host of cross-site scripting possibilities with specially crafted input to a variety of fields. This issue is patched in version 5.11.0. There are no known workarounds aside from upgrading.

CVE-2021-41132 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: ome - omero-web version < 5.11.0

CVSS3 Score: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
<b>NETWORK</b>	<b>LOW</b>	<b>NONE</b>	<b>REQUIRED</b>
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
<b>CHANGED</b>	<b>LOW</b>	<b>LOW</b>	<b>NONE</b>

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
<b>NETWORK</b>	<b>MEDIUM</b>	<b>NONE</b>
Confidentiality Impact	Integrity Impact	Availability Impact
<b>NONE</b>	<b>PARTIAL</b>	<b>NONE</b>

## CVE References

Description	Type	Link
-------------	------	------

Description	Tags	Link
Fix issues with inconsistency in input sanitisation leading to XSS ve... · ome/omero-web@0168067 · GitHub	<a href="#">github.com</a> <a href="#">text/html</a>	MISC <a href="https://github.com/ome/omero-web/commit/0168067accde5e635341b3c714b1d53ae92ba424">github.com/ome/omero-web/commit/0168067accde5e635341b3c714b1d53ae92ba424</a>
Inconsistent input sanitization leads to XSS vectors · Advisory · ome/omero-web · GitHub	<a href="#">github.com</a> <a href="#">text/html</a>	CONFIRM <a href="https://github.com/ome/omero-web/security/advisories/GHSA-g67g-hvc3-xmvf">github.com/ome/omero-web/security/advisories/GHSA-g67g-hvc3-xmvf</a>
2021-SV3 XSS vectors   Open Microscopy Environment (OME)	<a href="https://www.openmicroscopy.org">www.openmicroscopy.org</a> <a href="#">text/html</a>	MISC <a href="https://www.openmicroscopy.org/security/advisories/2021-SV3/">www.openmicroscopy.org/security/advisories/2021-SV3/</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).

### Related QID Numbers

980414 Python (pip) Security Update for omero-figure (GHSA-g67g-hvc3-xmvf)

### Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Openmicroscopy</a>	<a href="#">Omero-figure</a>	All	All	All	All
Application	<a href="#">Openmicroscopy</a>	<a href="#">Omero-web</a>	All	All	All	All

cpe:2.3:a:openmicroscopy:omero-figure:\*:\*:\*:\*:\*:\*:

cpe:2.3:a:openmicroscopy:omero-web:\*:\*:\*:\*:\*:\*:

No vendor comments have been submitted for this CVE

### Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-41132 : OMERO.web provides a web based client and plugin infrastructure. In versions prior to 5.11.0, a va... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2021-10-14 15:51:25

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2021 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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](https://status.cve.report)