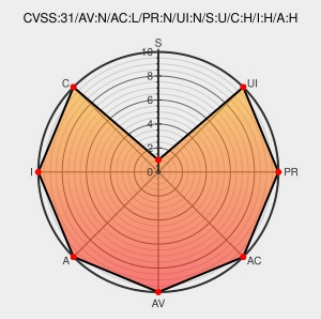
CVE-2021-41132

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



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
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	NONE

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link

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

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	Openmicroscopy	Omero-figure	All	All	All	All
Application	Openmicroscopy	Omero-web	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… twitter.com/i/web/status/1…	2021-10-14 15:51:25

← Previous ID

Next ID→