



CVE-2021-41110

Published on: 10/01/2021 12:00:00 AM UTC

Last Modified on: 10/08/2021 04:21:00 PM UTC

CVE-2021-41110 - advisory for GHSA-7g7j-f5g3-fqp7

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Cwlviewer](#) from [Commonwl](#) contain the following vulnerability:

cwlviewer is a web application to view and share Common Workflow Language workflows. Versions prior to 1.3.1 contain a Deserialization of Untrusted Data vulnerability. Commit number f6066f09edb70033a2ce80200e9fa9e70a5c29de (dated 2021-09-30) contains a patch. There are no available workarounds aside from

installing the patch. The SnakeYaml constructor, by default, allows any data to be parsed. To fix the issue the object needs to be created with a `SafeConstructor` object, as seen in the patch.

CVE-2021-41110 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: common-workflow-language - cwlviewer version < 1.3.1

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
CWL Viewer: deserialization of untrusted data can lead to complete takeover by an attacker · Advisory · common-workflow-language/cwlviewer · GitHub	github.com text/html	 CONFIRM github.com/common-workflow-language/cwlviewer/security/advisories/GHSA-7g7j-f5g3-fqp7
Analysis of the SnakeYaml deserialization in Java Security	www.fatalerrors.org text/html	 MISC www.fatalerrors.org/a/analysis-of-the-snakeyaml-deserialization-in-java-security.html
Use Yaml SafeConstructor (#355) · common-workflow-language/cwlviewer@f6066f0 · GitHub	github.com text/html	 MISC github.com/common-workflow-language/cwlviewer/commit/f6066f09edb70033a2ce80200e9fa9e70a5c29de

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Commonwl	Cwlviewer	All	All	All	All
cpe:2.3:a:commonwl:cwlviewer:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @kinow	CVE-2021-41110 "CWL Viewer: deserialization of untrusted data can lead to complete takeover by an attacker"... twitter.com/i/web/status/1...	2021-09-30 22:25:54
 @CVEreport	CVE-2021-41110 : cwlviewer is a web application to view and share Common Workflow Language workflows. Versions prio... twitter.com/i/web/status/1...	2021-10-01 12:26:18
 @threatmeter	CVE-2021-41110 cwlviewer is a web application to view and share Common Workflow Language workflows. Versions prior... twitter.com/i/web/status/1...	2021-10-02 07:09:43

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

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