



CVE-2021-29620

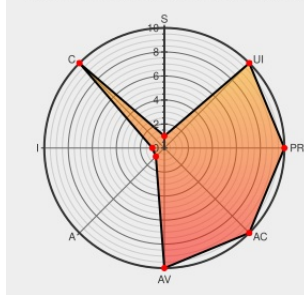
Published on: 06/23/2021 12:00:00 AM UTC

Last Modified on: 06/30/2021 12:56:00 AM UTC

CVE-2021-29620 - advisory for GHSA-24wf-7vf2-pv59

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

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



Certain versions of [Service-api](#) from [Reportportal](#) contain the following vulnerability:

Report portal is an open source reporting and analysis framework. Starting from version 3.1.0 of the service-api XML parsing was introduced. Unfortunately the XML parser was not configured properly to prevent XML external entity (XXE) attacks. This allows a user to import a specifically-crafted XML file which imports external Document

Type Definition (DTD) file with external entities for extraction of secrets from Report Portal service-api module or server-side request forgery. This will be resolved in the 5.4.0 release.

CVE-2021-29620 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [reportportal](#) - **reportportal** version **>= 3.1.0, < 5.4.0**

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
EMRPP-62610 Sax parser fix by Yumfriez · Pull Request #1392 · reportportal/service-api · GitHub	github.com text/html	MISC github.com/reportportal/service-api/pull/1392
XXE vulnerability on Launch import with externally-defined DTD file · Advisory · reportportal/reportportal · GitHub	github.com text/html	CONFIRM github.com/reportportal/reportportal/security/advisories/GHSA-24wf-7vf2-pv59
Please Wait... Cloudflare	mvnrepository.com text/html Inactive Link Not Archived	MISC mvnrepository.com/artifact/com.epam.reportportal/service-api

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.

Related QID Numbers

[982050](#) Java (maven) Security Update for com.epam.reportportal:service-api (GHSA-24wf-7vf2-pv59)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Reportportal	Service-api	All	All	All	All
cpe:2.3:a:reportportal:service-api:*****:*						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-29620 : Report portal is an open source reporting and analysis framework. Starting from version 3.1.0 of t... twitter.com/i/web/status/1...	2021-06-23 17:38:26
@threatmeter	CVE-2021-29620 Report portal is an open source reporting and analysis framework. Starting from version 3.1.0 of the... twitter.com/i/web/status/1...	2021-06-24 07:10:35
@SecRiskRptSME	RT: CVE-2021-29620 Report portal is an open source reporting and analysis framework. Starting from version 3.1.0 o... twitter.com/i/web/status/1...	2021-06-24 07:36:25
/r/netcve	CVE-2021-29620	2021-06-23 18:41:47

[← 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](#)