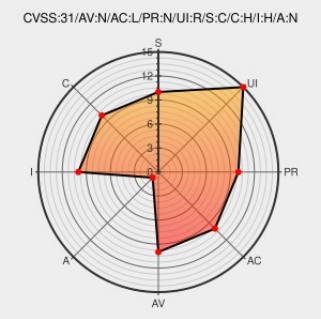
CVE-2020-15232

Published on: 10/02/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:42 PM UTC

CVE-2020-15232 - advisory for GHSA-vjv6-gq77-3mjw

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Print from Mapfish contain the following vulnerability:

In mapfish-print before version 3.24, a user can do to an XML External Entity (XXE) attack with the provided SDL style.

CVE-2020-15232 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **mapfish** - **mapfish-print** version **< 3.24**

CVSS3 Score: 9.1 - CRITICAL

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

CVSS2 Score: 6.4 - MEDIUM

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

CVE References

Description	Tags	Link
Fix some security issues by sbrunner · Pull Request #1397 · mapfish/mapfish-	Patch Third Party Advisory	MISC github.com/mapfish/mapfish-print/pull/1397/commits/e1d0527d13db06b2b62ca7d6afb9e97dacd67a0e

print · GitHub	Third Party Advisory github.com text/html	
Untrusted XML files · Advisory · mapfish/mapfish-print · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/mapfish/mapfish-print/security/advisories/GHSA-vjv6-gq77-3mjw

Related QID Numbers

983187 Java (maven) Security Update for org.mapfish.print:print-standalone (GHSA-vjv6-gq77-3mjw)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mapfish	Print	All	All	All	All
Application	Mapfish	Print	All	All	All	All

cpe:2.3:a:mapfish:print:*:*:*:*:*:*:*:*:

cpe:2.3:a:mapfish:print:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→