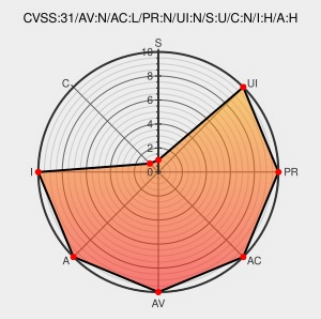
CVE-2022-37865

Published on: Not Yet Published

Last Modified on: 07/04/2023 03:15:00 AM UTC

CVE-2022-37865

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



Certain versions of Ivy from Apache contain the following vulnerability:

With Apache Ivy 2.4.0 an optional packaging attribute has been introduced that allows artifacts to be unpacked on the fly if they used pack200 or zip packaging. For artifacts using the "zip", "jar" or "war" packaging Ivy prior to 2.5.1 doesn't verify the target path when extracting the archive. An archive containing absolute paths or paths that try to traverse "upwards" using ".." sequences can then write files to any location on the local fie system that the user executing Ivy has write access to. Ivy users of version 2.4.0 to 2.5.0 should upgrade to Ivy 2.5.1.

CVE-2022-37865 has been assigned by security@apache.org to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **Apache Software Foundation** - **Apache Ivy** version **>= 2.4.0**

Affected Vendor/Software: **Apache Software Foundation** - **Apache Ivy** version **<= 2.5.0**

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	NONE	HIGH	HIGH

CVE References

Description	Tags	Link
No Description Provided	lists.apache.org text/html	MISC lists.apache.org/thread/gqvvv7qsm2dfjg6xzsw1s2h08tbr0sdy
[SECURITY] Fedora 38 Update: apache-ivy-2.5.1-3.fc38 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2023-35f775fd6e

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

284128 Fedora Security Update for apache (FEDORA-2023-35f775fd6e)

355182 Amazon Linux Security Advisory for apache-ivy : ALAS2023-2023-174

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Ivy	All	All	All	All

cpe:2.3:a:apache:ivy:*:*:*:*:*:*:*:*:

Discovery Credit

This issue was discovered by Kostya Kortchinsky of the Databricks Security Team.

Social Mentions

Source	Title	Posted (UTC)
/r/netcve	CVE-2022-37865	2022-11-07 11:38:20

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report