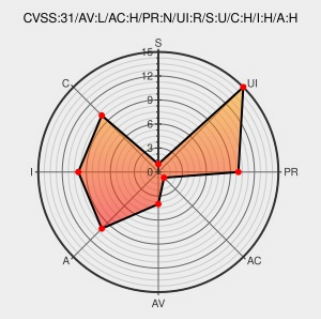
CVE-2022-44749

Published on: Not Yet Published

Last Modified on: 11/30/2022 07:48:00 PM UTC

CVE-2022-44749

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



Certain versions of Knime Analytics Platform from Knime contain the following vulnerability:

A directory traversal vulnerability in the ZIP archive extraction routines of KNIME Analytics Platform 3.2.0 and above can result in arbitrary files being overwritten on the user's system. This vulnerability is also known as 'Zip-Slip'. An attacker can create a KNIME workflow that, when being opened by a user, can overwrite arbitrary files that the user has write access to. It's not necessary to execute the workflow, opening the workflow is sufficient. The user will notice that something is wrong because an error is being reported but only after the files have already been written. This can impact data integrity (file contents are changed) or cause errors in other software (vital files being corrupted). It can even lead to remote code execution if executable files are being replaced and subsequently executed by the user. In all cases the attacker has to know the location of files on the user's system, though.

CVE-2022-44749 has been assigned by security@knime.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **KNIME** - **KNIME Analytics Platform** version **= 4.5.0**

Affected Vendor/Software: **KNIME** - **KNIME Analytics Platform** version **= 4.6.0**

Affected Vendor/Software: **KNIME** - **KNIME Analytics Platform** version **= 3.2.0**

CVSS3 Score: 7 - HIGH

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

CVE References

Description	Tags	Link
Security Advisories | KNIME	www.knime.com text/html	MISC www.knime.com/security/advisories

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	Knime	Knime Analytics Platform	All	All	All	All

cpe:2.3:a:knime:knime_analytics_platform:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-44749 : A directory traversal vulnerability in the ZIP archive extraction routines of KNIME Analytics Plat… twitter.com/i/web/status/1…	2022-11-24 07:07:24
/r/netcve	CVE-2022-44749	2022-11-24 08:38:39

← Previous ID

Next ID→

© CVE.report 2022 |
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 registred 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