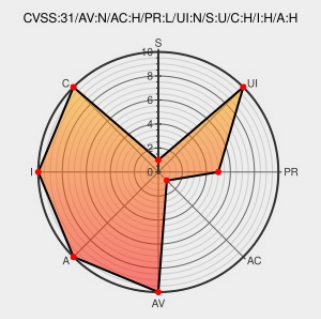
CVE-2022-44748

Published on: Not Yet Published

Last Modified on: 11/30/2022 07:38:00 PM UTC

CVE-2022-44748

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



Certain versions of Knime Server from Knime contain the following vulnerability:

A directory traversal vulnerability in the ZIP archive extraction routines of KNIME Server since 4.3.0 can result in arbitrary files being overwritten on the server's file system. This vulnerability is also known as 'Zip-Slip'. An attacker can create a KNIME workflow that, when being uploaded, can overwrite arbitrary files that the operating system user running the KNIME Server process has write access to. The user must be authenticated and have permissions to upload files to KNIME Server. 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 KNIME Server process user. In all cases the attacker has to know the location of files on the server's file system, though. Note that users that have permissions to upload workflows usually also have permissions to run them on the KNIME Server and can therefore already execute arbitrary code in the context of the KNIME Executor's operating system user. There is no workaround to prevent this vulnerability from being exploited. Updates to fixed versions 4.13.6, 4.14.3, or 4.15.3 are advised.

CVE-2022-44748 has been assigned by security@knime.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **KNIME** - **KNIME Server** version **= 4.15.0**

Affected Vendor/Software: **KNIME** - **KNIME Server** version **= 4.14.0**

Affected Vendor/Software: **KNIME** - **KNIME Server** version **= 4.3.0**

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	LOW	NONE
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 Server	All	All	All	All

cpe:2.3:a:knime:knime_server:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-44748 : A directory traversal vulnerability in the ZIP archive extraction routines of KNIME Server since 4… twitter.com/i/web/status/1…	2022-11-24 07:06:59
/r/netcve	CVE-2022-44748	2022-11-24 08:38:38

← Previous ID

Next ID→

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