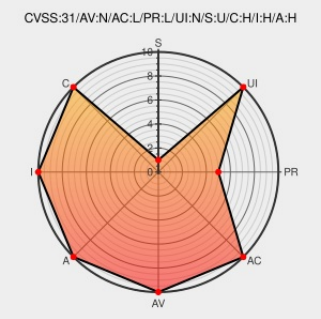
CVE-2020-8429

Published on: 02/11/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-8429

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



Certain versions of Kinetica from Kinetica contain the following vulnerability:

The Admin web application in Kinetica 7.0.9.2.20191118151947 does not properly sanitise the input for the function getLogs. This lack of sanitisation could be exploited to allow an authenticated attacker to run remote code on the underlying operating system. The logFile parameter in the getLogs function was used as a variable in a command to read log files; however, due to poor input sanitisation, it was possible to bypass a replacement and break out of the command.

CVE-2020-8429 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 9 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Release Notes	Release Notes	MISC support.kinetica.com/hc/en-us/categories/360001223653-Release-Notes

Release Notes – Kinetica	Release Notes Vendor Advisory web.archive.org text/html Inactive Link Not Archived	MISC support.kinetica.com/hc/en-us/categories/360001223653-Release-Notes
No Description Provided	Exploit Third Party Advisory www.nccgroup.trust text/html	MISC www.nccgroup.trust/uk/our-research/technical-advisory-command-injection/?research=Technical+advisories

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kinetica	Kinetica	7.0.9.2.20191118151947	All	All	All
Application	Kinetica	Kinetica	7.0.9.2.20191118151947	All	All	All

cpe:2.3:a:kinetica:kinetica:7.0.9.2.20191118151947:*:*:*:*:*:*:*:

cpe:2.3:a:kinetica:kinetica:7.0.9.2.20191118151947:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→