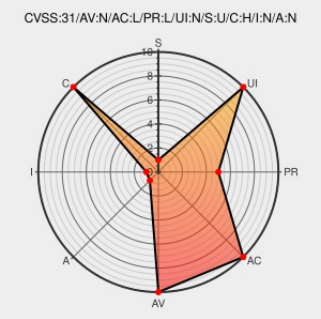
CVE-2019-13021

Published on: 05/14/2020 12:00:00 AM UTC

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

CVE-2019-13021

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



Certain versions of Jetselect from Jetstream contain the following vulnerability:

The administrative passwords for all versions of Bond JetSelect are stored within an unprotected file on the filesystem, rather than encrypted within the MySQL database. This backup copy of the passwords is made as part of the installation script, after the administrator has generated a password using ENCtool.jar (see CVE-2019-13022). This allows any low-privilege user who can read this file to trivially obtain the passwords for the administrative accounts of the JetSelect application. The path to the file containing the encoded password hash is /opt/JetSelect/SFC/resources/sfc-general-properties.

CVE-2019-13021 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 4 - MEDIUM

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

CVE References

Description	Tags	Link
CVE-2019-13021, 22, 23: JETSELECT Network Segregation Application - Nettitude Labs	Exploit Third Party Advisory labs.nettitude.com text/html	MISC labs.nettitude.com/blog/cve-2019-13021-22-23-jetselect-network-segregation-application/

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jetstream	Jetselect	All	All	All	All
Application	Jetstream	Jetselect	All	All	All	All

cpe:2.3:a:jetstream:jetselect:*:*:*:*:*:*:*:*:

cpe:2.3:a:jetstream:jetselect:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→