



CVE-2021-46398

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2021-46398
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-02-04 16:15:00 UTC
Updated	2022-03-04 16:39:00 UTC
Description	A Cross-Site Request Forgery vulnerability exists in Filebrowser < 2.18.0 that allows attackers to create a backdoor user wi

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Filebrowser	Filebrowser	All	All	All	All

References

Reference	Source	Link
fix: security issue in command runner (closes #1621) · filebrowser/filebrowser@74b7cd8 · GitHub	MISC	github.com
Critical CSRF in FileBrowser	MISC	febin0x4e4a.blogspot.com
FileBrowser 2.17.2 Code Execution / Cross Site Request Forgery ≈ Packet Storm	MISC	packetstormsecurity.com
Critical CSRF in FileBrowser febinNJ	MISC	febin0x4e4a.wordpress.com
CVE-2021-46398 Critical CSRF to RCE in FileBrowser by Febin Jan, 2022 System Weakness	MISC	febinj.medium.com
Critical CSRF to RCE in FileBrowser by Febin Jan, 2022 System Weakness	MISC	systemweakness.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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 registered 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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)