An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2607210267

NCSC Advisory

Critical Vulnerbilities in Progress ShareFile Storage Zones Controller

CVE-2026-2701 and CVE-2026-2699

21st, July 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

CVE ID: CVE-2026-2701

Published: 2026-04-02

Vendor: Progress

Product: ShareFile Storage Zones Controller

CVSS Score[1]: 9.1

Products Affected

Product	Version
ShareFile Storage Zones Controller	0 <= 5.12.3

Impact

An authenticated user can upload a malicious file to the server and execute it, which leads to remote code execution.

Common Weakness Enumeration (CWE)[2]: CWE-434: Unrestricted Upload of File with Dangerous Type, CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), CWE-94: Improper Control of Generation of Code ('Code Injection')

Known Exploited Vulnerability (KEV) catalog[3]: No

Used by Ransomware Operators: N/A

[1] https://www.first.org/cvss/
[2] https://cwe.mitre.org
[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Description

CVE ID: CVE-2026-2699

Published: 2026-04-02

Vendor: Progress

Product: ShareFile Storage Zones Controller

CVSS Score[4]: 9.8

Products Affected

Product	Version
ShareFile Storage Zones Controller	0 <= 5.12.3

Impact

Customer Managed ShareFile Storage Zones Controller (SZC) allows an unauthenticated attacker to access restricted configuration pages. This leads to changing system configuration and potential remote code execution.

Common Weakness Enumeration (CWE)[5]: CWE-698: Execution After Redirect (EAR), CWE-284: Improper Access Control

Known Exploited Vulnerability (KEV) catalog[6]: No

Used by Ransomware Operators: N/A

[4] https://www.first.org/cvss/
[5] https://cwe.mitre.org
[6] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Progress.

CVE-2026-2701:

- https://nvd.nist.gov/vuln/detail/CVE-2026-2701
- https://www.cve.org/CVERecord?id=CVE-2026-2701
- https://docs.sharefile.com/en-us/storage-zones-controller/5-0/security-vulnerability-feb26

CVE-2026-2699:

- https://nvd.nist.gov/vuln/detail/CVE-2026-2699
- https://www.cve.org/CVERecord?id=CVE-2026-2699
- https://docs.sharefile.com/en-us/storage-zones-controller/5-0/security-vulnerability-feb26