RCE vulnerability in Progress ShareFile Storage Zones Controller (SZC)

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-2701
State	PUBLISHED
Assigner	ProgressSoftware
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-02 14:16:27 UTC
Updated	2026-04-21 00:28:12 UTC
Description	Authenticated user can upload a malicious file to the server and execute it, which leads to remote code execution.

Risk And Classification

Primary CVSS: v3.1 8.8 HIGH from nvd@nist.gov

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.001900000 probability, percentile 0.408150000 (date 2026-04-07)

Problem Types: CWE-78 | CWE-94 | CWE-434 | CWE-434 CWE-434: Unrestricted Upload of File with Dangerous Type | CWE-78 CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | CWE-94 CWE-94: Improper Control of Generation of Code ('Code Injection')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	security@progress.com	Secondary	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
3.1	CNA	CVSS	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Progress	Sharefile Storage Zones Controller	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Progress	ShareFile Storage Zones Controller	affected 5.12.3 semver	Not specified

References

Reference	Source	Link	Tags
docs.sharefile.com/en-us/storage-zones-controller/5-0/security-vulnerability-feb26	security@progress.com	docs.sharefile.com	Vendor A
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

Vendor Comments And Credit

Discovery Credit

CNA: Piotr Bazydlo of watchTowr (en)

Additional Advisory Data

Workarounds

CNA: Reset the secret and password using custom tool provided by ShareFile

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**