AUTORITETI KOMBËTAR

PËR SIGURINË KIBERNETIKE

Dobësi të Shumta në Progress ShareFile që Mundësojnë Ekzekutim në Distancë të Kodit (RCE)

Data: 03/04/2026
Version: 1.0

Përmbajtja

Përmbledhje Ekzekutive 1
Informacione Teknike 1
Rekomandime 2
Referenca 2

Përmbledhje Ekzekutive

Janë identifikuar disa dobësi kritike në Progress ShareFile që mund të çojnë në ekzekutim në distancë të kodit dhe kompromet im të plotë të serverit.

Informacione Teknike

Detaje të Dobësive:

Dobësitë lidhen me një kombinim të:

- anashkalimit të autentikimit
- mekanizmit të pasaktë të trajtimit të skedarëve

Këto së bashku u mundësojnë sulmuesve të ngarkojnë dhe ekzekutojnë **ASPX web shells** keqdashëse në webroot të aplikacionit.

Gjithashtu, janë publikuar **proof-of-concept (PoC)** për CVE-të përkatëse, duke rritur ndjeshëm rrezikun e shfrytëzimit.

1. Anashkalim i Autentikimit – CVE-2026-2699 (9.8 Kritike)

- Komponenti: Storage Zones Controller (SZC)
- Tipi: Anashkalim autentikimi përmes trajtimit të pasaktë të ridrejtimit HTTP
- Ndikimi: Akses i paautorizuar në ndërfaqen administrative të ShareFile
- Vektori i sulmit: Shfrytëzimi i logjikës së ridrejtimit për të anashkaluar kontrollet e autentikimit

2. Ekzekutim në Distancë i Kodit – CVE-2026-2701 (9.1 Kritike)

- Komponenti: Storage Zones Controller (SZC)
- Tipi: RCE përmes abuzimit të ngarkimit të skedarëve
- Ndikimi: Kompromet im i plotë i serverit
- Vektori i sulmit:
  - Abuzim i funksionalitetit të ngarkimit dhe ekstraktimit të skedarëve
  - Vendosje e web shell-eve ASPX në webroot
  - Ekzekutim i kodit arbitrar në server

Sistemet e Prekura

- Versionet e Progress ShareFile më të hershme se **5.12.4**
- Implementimet që përdorin komponentin **Storage Zones Controller (SZC)**

Versionet e Korrigjuara

- Progress ShareFile **5.12.4**

Rekomandime

Rekomandohet të:

- Përditësoni Progress ShareFile në versionin e korrigjuar ose më të fundit
- Aplikoni menjëherë patch-et për të gjitha instancat e ekspozuara të SZC
- Kufizoni ekspozimin publik të komponentëve SZC sa herë që është e mundur

Referenca

https://www.cve.org/CVERecord?id=CVE-2026-2699
https://www.cve.org/CVERecord?id=CVE-2026-2701