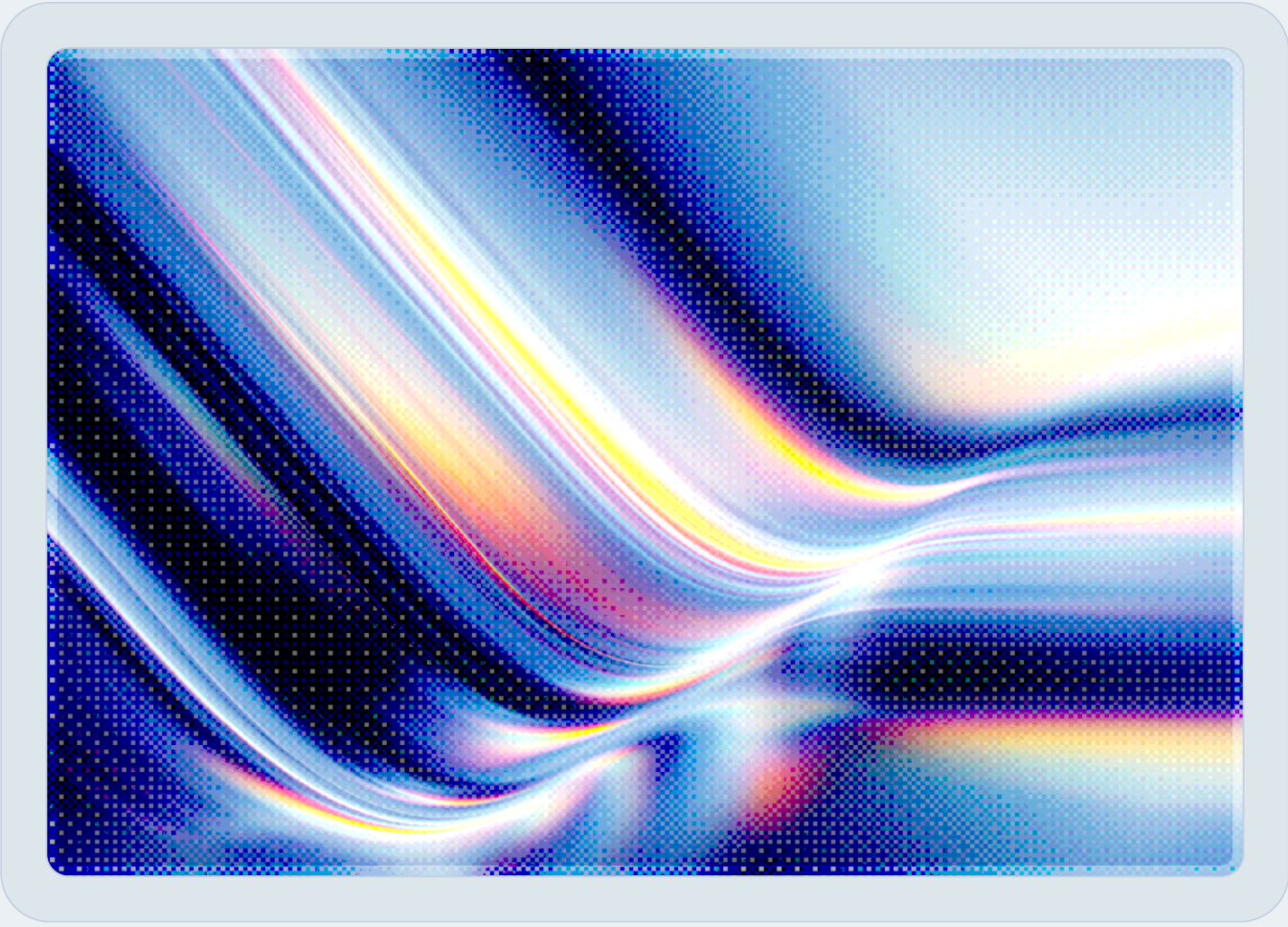
CSAI Foundation | Cloud Security Alliance

ShareFile's Credible Threat: A Pre-Auth RCE Chain Explained

2026-07-14

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

Key Takeaways

On July 10, 2026, Progress Software told every customer running a ShareFile Storage Zone Controller (SZC) to physically power down the Windows server hosting it, citing a "credible external security threat" it declined to describe further [1][2]. The company disabled cloud-side account access for hybrid deployments as a precaution and, as of this writing, has not confirmed whether any customer has actually been compromised [2][3]. Independent researchers and the Shadowserver Foundation have connected the dots that Progress would not: honeypots began recording live exploitation attempts against CVE-2026-2699, an authentication-bypass flaw in SZC that watchTowr Labs disclosed in April 2026 and Progress patched in version 5.12.4 [4][8]. That flaw chains with a second bug, CVE-2026-2701, to grant an unauthenticated attacker full remote code execution on the server, with no credentials, phishing, or user interaction required [5]. Roughly 784 SZC instances were directly reachable from the internet at last count, though a broader watchTowr scan found nearly 30,000 ShareFile-related endpoints exposed in total, and only the older 5.x branch is vulnerable; the newer, .NET Core–based 6.x line is unaffected [4][5]. For security teams, this incident illustrates how a vulnerability chain that was publicly disclosed and already patched months earlier can still trigger an emergency full-shutdown order once attackers begin actively probing for it in the wild.

Background

ShareFile is Progress Software's enterprise file-sharing and sync platform, used widely by accounting firms, law offices, healthcare providers, and other organizations that need to exchange sensitive documents with external parties under contractual or regulatory retention requirements. Many ShareFile customers do not store data purely in Progress's cloud; instead, they deploy a Storage Zone Controller, a self-hosted Windows component that lets an organization keep file storage on its own infrastructure, typically to satisfy data residency, HIPAA, or client-contract requirements, while still using ShareFile's cloud-hosted control plane for authentication, sharing, and workflow. This hybrid architecture is common across regulated industries specifically because it lets a firm say "the data never leaves our network," even though the service is administered and billed through Progress's SaaS backend.

That architecture has been targeted by unauthenticated RCE vulnerabilities before. In 2023, a separate unauthenticated RCE vulnerability in Storage Zone Controllers, CVE-2023-24489, was actively exploited while ShareFile was still owned by Citrix, before Progress's 2024 acquisition of the product line [3]. Progress Software's broader product portfolio has also been the source of some of the industry's highest-profile mass-exploitation events, including the 2023 MOVEit Transfer campaign, in which the Cl0p ransomware group exploited a SQL injection flaw in a conceptually similar managed-file-transfer product to compromise thousands of organizations, prompting a joint CISA-FBI advisory [9]. Progress's file-transfer and file-sharing product lines have consequently become a recurring subject of security research, and watchTowr Labs, a commercial vulnerability research firm known for extensively documenting exploitation chains in enterprise file-transfer software, took a close look at Storage Zone Controller in early 2026.

In April 2026, watchTowr disclosed two chainable vulnerabilities it had found in SZC's 5.x branch: CVE-2026-2699 (CVSS 9.8), tracked internally as WT-2026-0006, and CVE-2026-2701 (CVSS 9.1), tracked as WT-2026-0007 [4][5]. Progress shipped a fix in version 5.12.4, released March 10, 2026, and confirmed that the newer 6.x branch, a full rewrite on .NET Core, was never affected [5]. Measured from the April disclosure to the July shutdown order, the chain had been public for roughly three months; measured from the March 10 patch, it had been available as a fix for roughly four months. Either way, the vulnerability sat in the public record for an extended stretch as a patched, disclosed-but-not-yet-weaponized issue, the kind of finding that typically prompts a routine patch cycle rather than an emergency response. That changed the week of July 6, when Progress's threat intelligence apparently detected signs of hostile activity serious enough to order every SZC customer, patched or not, to unplug their servers rather than wait for confirmation of compromise [1][2].

Security Analysis

How the chain works

The two vulnerabilities are best understood as a broken lock (CVE-2026-2699) followed by an open window behind it (CVE-2026-2701). CVE-2026-2699 is an authentication-bypass flaw classified under CWE-698 (Execution After Redirect). The SZC admin configuration endpoint, `/ConfigService/Admin.aspx`, does check whether a visitor is authenticated, and it does issue an HTTP redirect to the login page when they are not, but the redirect call passes `false` for its "end response" parameter. In ASP.NET, that parameter controls whether the server actually halts processing after sending the redirect; setting it to `false` means the server sends the visitor a 302 response pointing them to the login page, and then keeps executing the rest of the admin page's logic anyway, rendering the full administrative interface in the response body regardless of the redirect. An attacker who simply ignores the `Location` header, trivial to do with almost any scripting tool, receives the entire unauthenticated admin panel. Researchers noted a reliable fingerprint for this bug in server logs: a 302 response from that endpoint whose body still exceeds 10,000 characters, since a genuine redirect response should be nearly empty [5].

Reaching the admin panel without a password only sets up the second half of the chain. CVE-2026-2701 lives in how SZC validates the storage location an administrator can configure for a "zone." The validation logic only confirms that a location is writable, by creating and then deleting a small test file there; it never restricts which directory an admin is allowed to designate as a storage target in the first place. Because the bypassed admin panel lets an unauthenticated attacker reach that configuration screen, the attacker can point the "Network Share Location" setting directly at the server's own web root (in the researchers' proof of concept, `C:\inetpub\wwwroot\ShareFile\StorageCenter\documentum`), turning the file-upload feature into a mechanism for writing files that the web server will later execute. From there, the attacker uses SZC's own `/upload.aspx` endpoint with its `unzip=true` option, which extracts an uploaded ZIP archive's contents in place without renaming or stripping file extensions. Uploading a ZIP containing a web shell with an `.aspx` extension, then, deposits an executable script inside the web root, where a normal HTTP request will run it with the privileges of the ShareFile web application.

That upload endpoint is not entirely open, however; it requires a valid HMAC-SHA256 signature tied to the target storage zone. WatchTowr's research showed that this signature can also be forged without valid credentials: a related configuration API, `/ConfigService/api/StroageZoneConfig` (the misspelling appears in the product itself), leaks an encrypted value called `TempData2`, which can be decrypted using a hardcoded salt value baked into the SZC codebase. That decryption recovers the zone's secret key, which is exactly what is needed to compute a valid HMAC for the upload request. Chained end to end, an attacker with only network access to an internet-facing SZC instance can bypass authentication, redirect file storage into the web root, forge the signature required to upload there, and drop a web shell, all without a username, password, or any interaction from a legitimate user. Table 1 summarizes the chain.

Stage	Vulnerability	Mechanism	Outcome
1. Auth bypass	CVE-2026-2699 (CWE-698, CVSS 9.8)	`Response.Redirect()` called with `endResponse=false`; page logic executes after the 302	Unauthenticated access to `/ConfigService/Admin.aspx`
2. Signature forgery	Related to CVE-2026-2701	`TempData2` leaked via `/ConfigService/api/StroageZoneConfig`, decrypted with a hardcoded salt	Valid HMAC-SHA256 for upload requests
3. Path manipulation	CVE-2026-2701 (CVSS 9.1)	Zone storage validation only checks writability, not directory scope	Storage location redirected into the IIS web root

Stage	Vulnerability	Mechanism	Outcome
4. Code execution	CVE-2026-2701	`/upload.aspx?unzip=true` extracts ZIP contents in place, preserving extensions	ASPX web shell written to a web-reachable path and executed

Why a patched, months-old bug is triggering an emergency shutdown

Progress's own public statements about the July incident have been notably decoupled from the CVE-2026-2699/2701 disclosure: the company has said only that it identified a "credible external security threat" and has not confirmed the two are related [3][6]. But the independent evidence points in that direction. Shadowserver's honeypots began recording active exploitation attempts specifically against CVE-2026-2699 in the days before Progress's shutdown order, tying the current activity to the April disclosure [8]. If accurate, this reflects a pattern documented repeatedly in enterprise file-transfer and file-sharing software: a vendor patches a critical, pre-auth RCE chain, disclosure details eventually become public (or are independently rediscoverable from the patch diff), and attackers who skipped the vulnerability the first time around take a second look once it is clear which organizations never applied the fix. The gap between "patch available" and "organization actually patched" is where this kind of exploitation lives, and it is precisely the gap that CSA's research on vulnerability data quality has flagged as a systemic weakness in how the industry currently tracks and communicates exploitation risk over a vulnerability's full lifecycle, rather than just at the moment of disclosure [7].

The severity of Progress's response, ordering a full server shutdown rather than simply pushing another patch, narrows the plausible explanations to two: either the vendor cannot rule out that some fraction of its installed base is running an unpatched or misconfigured version despite the March fix being months old, or the "credible threat" involves indicators of compromise, stolen credentials, or attacker tooling that a version upgrade alone would not remediate. Which of these is closer to the truth has not been resolved publicly as of this writing, and organizations should treat both possibilities as live until Progress says otherwise.

Exposure and blast radius

The exposure figures reported by different researchers vary because they measured different things. Shadowserver's count of roughly 784 internet-reachable SZC instances reflects hosts fingerprinted specifically as Storage Zone Controllers; watchTowr's much larger figure of nearly 30,000 reflects a broader scan of ShareFile-related web endpoints, which likely includes cloud-hosted ShareFile accounts that do not run a self-managed SZC and are therefore not exposed to this particular chain [4][5]. The meaningfully at-risk population is closer to the smaller figure: organizations running a customer-managed SZC on the 5.x branch, reachable from the internet, and not yet upgraded to 5.12.4. Because SZC is disproportionately deployed by organizations with data-residency or regulatory reasons for keeping storage on-premises, that population likely skews toward sectors such as legal, healthcare, financial services, and government contracting, where a successful compromise carries outsized breach-notification and client-confidentiality consequences, independent of the raw instance count.

Recommendations

Immediate Actions

Organizations running any ShareFile Storage Zone Controller should treat Progress's shutdown guidance as authoritative until the company confirms the investigation is closed, since the vendor's own communications indicate the threat may extend beyond the two disclosed CVEs. Security teams should independently verify their SZC version against 5.12.4 or the 6.x branch, and should search IIS logs for the CVE-2026-2699 fingerprint described above: 302 responses from `/ConfigService/Admin.aspx` with response bodies exceeding roughly 10,000 characters, as well as any unexpected `.aspx` files under the web root or ZIP uploads containing executable script extensions.

Short-Term Mitigations

Once Progress confirms it is safe to bring servers back online, organizations should upgrade directly to the 6.x branch where feasible rather than remaining on 5.x, since the architectural rewrite eliminates this vulnerability class entirely rather than patching a specific instance of it. Where migration to 6.x is not immediately possible, SZC instances should be moved behind a reverse proxy or VPN that removes them from direct internet exposure, since the entire attack chain depends on unauthenticated network reachability to the admin and upload endpoints. Organizations should also rotate any zone secrets and API credentials associated with affected Storage Zone Controllers, given that the exploit chain's HMAC-forgery step depends on a static hardcoded salt value that cannot be changed through normal configuration.

Strategic Considerations

This incident is a useful prompt for revisiting how an organization tracks the gap between "patch available" and "patch applied" for internet-facing, vendor-managed components, a gap that is frequently invisible to central IT because Storage Zone Controllers and similar edge appliances are often deployed and maintained by a business unit rather than the security team. Programs relying on self-hosted extensions of SaaS platforms should periodically re-verify exposure and patch status independent of vendor attestations, particularly for products with a history of exploited RCE chains, and should weight exploitation-in-the-wild intelligence rather than CVSS score alone when prioritizing which "already patched" vulnerabilities warrant renewed urgency months after disclosure.

CSA Resource Alignment

CSA's Top Concerns with Vulnerability Data speaks directly to a dynamic visible in this incident: a static CVSS score assigned at disclosure time (9.8 and 9.1 for CVE-2026-2699 and CVE-2026-2701, respectively) captured the technical severity of the chain in April but said nothing about the exploitation timeline that would follow. The report's argument that vulnerability management programs need context-aware, exploitation-informed prioritization rather than a one-time CVSS snapshot is precisely what would have flagged this SZC chain for renewed attention the moment Shadowserver's honeypots recorded live attacks in July, months after the initial patch cycle had already concluded for most organizations.

As a topical fallback, the AI Controls Matrix (AICM v1.1) is relevant to organizations assessing this incident within a broader third-party and technology vulnerability management (TVM) program, even though this specific event does not involve AI systems: AICM's TVM domain controls around vendor patch management, exposure tracking, and vulnerability lifecycle governance apply equally to conventional on-premises software components such as Storage Zone Controller, and organizations building AI-inclusive control programs should ensure the same rigor is applied to legacy, non-AI infrastructure that remains part of the same trust boundary.

References

[1] The Hacker News. "URGENT - Progress Tells ShareFile Customers to Shut Down Storage Zone Controllers Over Security Threat." The Hacker News, July 2026.

[2] Bleeping Computer. "Progress urges ShareFile customers to shut down servers over "credible" threat." Bleeping Computer, July 10, 2026.

[3] Security Affairs. "Progress Told ShareFile Customers to Pull the Plug on Their Servers. Here's What We Know." Security Affairs, July 2026.

[4] Cybersecurity News. "Progress Urges ShareFile Admins to Shut Down Servers Over Credible Security Threat." Cybersecurity News, July 2026.

[5] watchTowr Labs. "You're Not Supposed to ShareFile with Everyone: Progress ShareFile Pre-Auth RCE Chain (CVE-2026-2699, CVE-2026-2701)." watchTowr Labs, April 2026.

[6] SecurityWeek. "Progress Prompts ShareFile Storage Zone Controller Shutdown Amid Security Concerns." SecurityWeek, July 2026.

[7] Cloud Security Alliance. "Top Concerns with Vulnerability Data." Cloud Security Alliance, 2024.

[8] BankInfoSecurity. "Progress Urges ShareFile Shutdown Over 'Credible' Threat." BankInfoSecurity, July 2026.

[9] CISA and FBI. "#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability." Cybersecurity and Infrastructure Security Agency, June 2023.