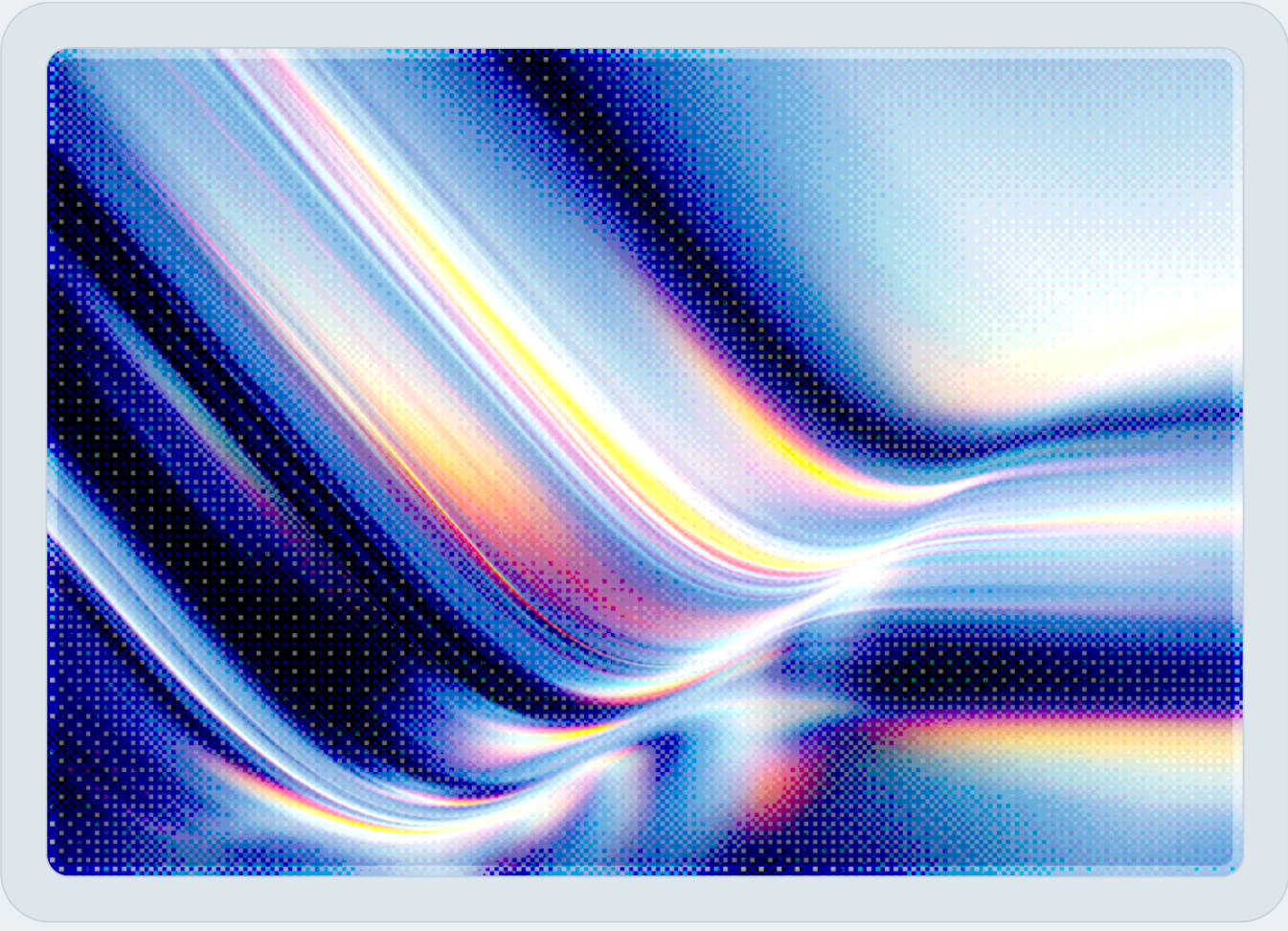
CSAI Foundation | Cloud Security Alliance

CVE-2026-45659: SharePoint RCE Under Active Exploitation

CISA's KEV Listing and the July 4 Federal Remediation Deadline

2026-07-03

AI-assisted Rapid Research



CSAI | cloud security alliance®

Key Takeaways

The Cybersecurity and Infrastructure Security Agency added CVE-2026-45659, a deserialization flaw in on-premises Microsoft SharePoint Server, to its Known Exploited Vulnerabilities catalog on July 1, 2026, after confirming active exploitation in the wild [1]. The listing carries a compressed remediation window: Federal Civilian Executive Branch agencies must apply the fix by July 4, 2026, under the risk-based patching requirements of Binding Operational Directive 26-04 [2]. Any organization running SharePoint Server Subscription Edition, SharePoint Server 2019, or SharePoint Enterprise Server 2016 faces the same exposure, since the flaw requires only low-privileged, authenticated access to achieve full remote code execution [3]. CSA recommends that these organizations treat the same three-day window CISA set for federal agencies as the practical deadline for their own environment, regardless of federal status.

What makes CVE-2026-45659 notable is not just its severity but the gap between Microsoft's original risk assessment and how events unfolded. When Microsoft patched the vulnerability in an out-of-band update on May 21, 2026, it rated exploitation "Less Likely" under its Exploitability Index, even though the same advisory scored the flaw's attack complexity as Low, meaning an attacker needed no special conditions or repeated attempts to succeed [4][5]. The two assessments are not contradictory on their face: Microsoft's Exploitability Index also weighs factors such as the absence of a public proof-of-concept and the authentication requirement, considerations a Low attack-complexity score alone does not capture. Roughly six weeks later, CISA confirmed the flaw was being exploited against real targets. The episode illustrates a real limitation of vendor exploitability predictions: they are probabilistic judgments made before an exploit exists, and they cannot fully anticipate how quickly one will surface once conditions such as available credentials and an unpatched population align, so patch prioritization decisions built solely on a vendor's initial severity language can leave organizations exposed during that interval.

The vulnerability also arrives against a backdrop that on-premises SharePoint administrators will find uncomfortably familiar. Eleven SharePoint vulnerabilities have been added to CISA's KEV catalog since 2021, and seven of those have been connected to ransomware deployment [4]. The most consequential prior episode, the "ToolShell" exploit chain disclosed in July 2025, combined an authentication bypass with a deserialization flaw to allow unauthenticated remote code execution against SharePoint Server, and was weaponized within days by Storm-2603, a China-based threat actor with a documented hybrid profile of ransomware deployment and suspected espionage activity, to compromise victims spanning finance, energy, healthcare, and government sectors, including at least one U.S. federal nuclear security entity [7][8]. CVE-2026-45659 does not require the same unauthenticated bypass, but the underlying

weakness class, insecure deserialization in SharePoint's server-side processing pipeline, is the same one that made ToolShell so damaging, which raises the question of whether SharePoint's architecture has a structural, recurring exposure rather than a series of unrelated bugs.

Background

Microsoft SharePoint Server remains one of the most widely deployed on-premises collaboration platforms in the enterprise and public sector, and its role as a document repository, intranet portal, and workflow engine means a compromised instance typically provides an attacker with broad access to internal files, credentials cached in connected services, and a foothold for lateral movement into the rest of the network. That combination of high privilege and high exposure has made on-premises SharePoint a recurring target for both financially motivated ransomware operators and nation-state actors over the past several years [4][7], a pattern that predates this specific vulnerability and that shaped how quickly CISA and the security community reacted once exploitation was confirmed.

CVE-2026-45659 was disclosed and patched by Microsoft on May 21, 2026, through an out-of-band security update issued after the fix was inadvertently left out of that month's regularly scheduled Patch Tuesday release [4]. The affected builds are SharePoint Server Subscription Edition prior to build 16.0.19725.20280, SharePoint Server 2019 prior to build 16.0.10417.20128, and SharePoint Enterprise Server 2016 prior to build 16.0.5552.1002 [5]. SharePoint Online, the software-as-a-service offering within Microsoft 365, is not affected; Microsoft patches its own multi-tenant infrastructure independently of the on-premises release cycle, and this vulnerability is scoped entirely to self-hosted deployments [3]. Organizations that have already migrated fully to SharePoint Online have no exposure to this particular flaw, but the substantial population of enterprises and government agencies that retain on-premises or hybrid SharePoint deployments, often for data residency, customization, or legacy integration reasons, remain squarely in scope.

CISA added the vulnerability to its Known Exploited Vulnerabilities catalog on July 1, 2026, citing reliable evidence of active exploitation, though the agency has not published details on the specific tactics, techniques, or threat actors involved [1][6]. That is a normal and deliberate posture for CISA: KEV entries are triggered by confirmed evidence of in-the-wild use, not by full incident attribution, and technical details are often withheld or delayed to avoid providing a roadmap to less sophisticated attackers while defenders are still patching. Independent scanning by the nonprofit Shadowserver Foundation identified more than 10,000 internet-facing SharePoint servers still reachable at the time of the KEV listing. That figure reflects overall exposure rather than confirmed patch status, since Shadowserver's scan did not

determine how many of those servers remain vulnerable versus already remediated, but it nonetheless indicates a large attack surface that defenders should assume is only partially patched given how recently the KEV listing occurred [4].

Security Analysis

CVE-2026-45659 carries a CVSS base score of 8.8, reflecting a network attack vector, low attack complexity, low privileges required, and no user interaction, combined with high impact to confidentiality, integrity, and availability [3][4]. In practical terms, an attacker who has obtained or purchased valid credentials for a SharePoint site, even credentials with nothing more than Site Member permissions and no administrative role, can send a crafted request that causes the server to deserialize attacker-controlled data and execute arbitrary code in the context of the SharePoint application pool. The requirement for authentication is a meaningful mitigating factor relative to an unauthenticated flaw like the 2025 ToolShell chain, but it is a modest one in practice: as a general industry pattern, low-privileged SharePoint accounts tend to be provisioned broadly across an organization's workforce and extranet partners, are frequently reused or weakly protected, and are a routine target of credential-stuffing and phishing campaigns, any of which could give an attacker exactly the access level this vulnerability requires.

Insecure deserialization vulnerabilities of this kind typically arise when an application accepts serialized object data from a client and reconstructs it into live objects without adequately validating or restricting what types of objects can be instantiated. If the application's runtime includes classes whose construction or destruction logic can be chained to execute arbitrary commands, so-called "gadget chains," an attacker who controls the serialized payload can trigger code execution the moment the server deserializes it. SharePoint's history includes at least two vulnerabilities in this class, including the deserialization component of the 2025 ToolShell chain, which suggests the platform's extensibility model, which relies heavily on serialization for workflow state, view state, and inter-component communication, may present a durable attack surface for this bug class specifically, even if not every historical SharePoint KEV entry shares this root cause.

The practical consequence of successful exploitation is severe. Remote code execution on a SharePoint server typically grants an attacker access to the server's file system, its connection strings and service account credentials, and often a trust relationship with Active Directory that can be leveraged for further privilege escalation. The ToolShell campaign demonstrated this progression directly: initial access through the SharePoint vulnerability was used to harvest ASP.NET machine keys, which in turn allowed attackers to forge authentication tokens and maintain persistent access even after the original vulnerability was patched, unless organizations also rotated the exposed keys [7]. Organizations

remediating CVE-2026-45659 should treat key and credential rotation as part of the response, not merely as an optional hardening step, particularly for any server where exploitation cannot be confidently ruled out.

The unresolved question, and one CISA has not yet answered publicly, is what class of actor is behind the current exploitation and what their objective is. The historical base rate for SharePoint KEV entries, seven of eleven tied to ransomware since 2021, suggests financially motivated extortion is a reasonable working hypothesis, but espionage-motivated access is equally plausible given SharePoint's role as a document repository in government and defense-adjacent organizations [4]. Absent public attribution, defenders should assume the exploitation could support either objective and prioritize detection and response accordingly, rather than tailoring their monitoring narrowly to a single threat model.

Recommendations

Immediate Actions

Organizations operating any of the affected on-premises SharePoint versions should apply Microsoft's May 21, 2026 out-of-band security update without waiting for a routine patch cycle, and should verify patch application against the specific build numbers Microsoft has published rather than relying on the presence of a more recent cumulative update alone [4][5]. Where patching cannot be completed within the 72-hour window CISA has effectively set through the KEV deadline, administrators should restrict network-level access to the SharePoint front end to known-good source ranges, disable or closely monitor site collections used by external partners, and review authentication logs for anomalous Site Member-level account activity as an interim compensating control. Given the ToolShell precedent, organizations should also rotate ASP.NET machine keys on affected SharePoint farms following the patch, since a key exposed prior to remediation would allow an attacker to retain forged-token access even after the underlying vulnerability is closed [7].

Short-Term Mitigations

Beyond the immediate patch, security teams should audit which accounts hold Site Member or higher permissions across their SharePoint environment and confirm that the principle of least privilege has been applied, since this vulnerability's practical exploitability depends heavily on how broadly low-privileged access has been provisioned. Multi-factor authentication should be enforced for all accounts with any SharePoint access, reducing the likelihood that credential theft alone is sufficient to reach the privilege level the exploit requires. Organizations should also confirm that endpoint detection and web

application firewall rules have been updated to reflect any published indicators of compromise as they become available from CISA, Microsoft, or established threat intelligence vendors, and should retain SharePoint and IIS logs for an extended window to support retrospective investigation if evidence of pre-patch exploitation surfaces later.

Strategic Considerations

The recurrence of serious, actively exploited vulnerabilities in on-premises SharePoint, eleven KEV entries since 2021, argues for organizations to treat self-hosted SharePoint as a persistently high-risk asset class deserving dedicated monitoring and an accelerated patch SLA, rather than folding it into a general enterprise patch cadence measured in weeks [4]. Organizations that have not yet evaluated migration to SharePoint Online should weigh the recurring cost of emergency patching, incident response, and credential rotation against the migration effort, particularly where data residency or customization requirements that originally justified on-premises deployment may have weakened over time. More broadly, the gap between Microsoft's initial "Exploitation Less Likely" rating and the confirmed exploitation six weeks later should inform how organizations calibrate patch prioritization: vendor exploitability assessments are a useful input but should be weighted alongside a vulnerability's technical characteristics, such as the low complexity and low privilege requirements present here, when deciding how urgently to act ahead of confirmed in-the-wild activity.

CSA Resource Alignment

CVE-2026-45659 is a conventional infrastructure vulnerability rather than an AI-specific risk, but it illustrates several control areas that CSA's frameworks address directly. The AI Controls Matrix and its predecessor Cloud Controls Matrix both include domains for vulnerability and patch management, identity and access management, and change control that map directly onto the recommendations above. Organizations that have implemented AICM-aligned controls are better positioned to identify affected SharePoint instances, since asset inventory and privileged-access visibility are core AICM control domains, though the speed of identification still depends on how completely those controls have been operationalized. CSA's Zero Trust guidance is relevant to the broader mitigating posture described here: continuous verification of authenticated sessions, rather than implicit trust after login, is one of several controls that can reduce, though not eliminate, the value of the low-privileged access this vulnerability requires. Organizations pursuing STAR certification or a STAR Level 2 assessment should expect vulnerability response timelines like this one, from disclosure to patch to KEV listing to

remediation deadline, to be scrutinized as evidence of operational maturity in their control implementation, and should ensure their incident response documentation captures the specific timeline and actions taken in response to CVE-2026-45659 if their environment was affected.

References

[1] Cybersecurity and Infrastructure Security Agency. "CISA Adds One Known Exploited Vulnerability to Catalog." CISA, July 1, 2026.

[2] Cybersecurity and Infrastructure Security Agency. "BOD 26-04: Prioritizing Security Updates Based on Risk." CISA.

[3] The Hacker News. "SharePoint RCE CVE-2026-45659 Added to CISA KEV After Active Exploitation." The Hacker News, July 2026.

[4] BleepingComputer. "CISA: Microsoft SharePoint RCE Flaw Now Actively Exploited." BleepingComputer, July 2, 2026.

[5] Help Net Security. "High-Severity SharePoint RCE Bug Patched by Microsoft (CVE-2026-45659)." Help Net Security, May 26, 2026.

[6] SecurityWeek. "CISA Warns of Actively Exploited Microsoft SharePoint Vulnerability." SecurityWeek, July 2026.

[7] Microsoft Security. "Disrupting Active Exploitation of On-Premises SharePoint Vulnerabilities." Microsoft Security Blog, July 22, 2025.

[8] Unit 42, Palo Alto Networks. "Active Exploitation of Microsoft SharePoint Vulnerabilities: Threat Brief." Unit 42, updated August 12, 2025.

