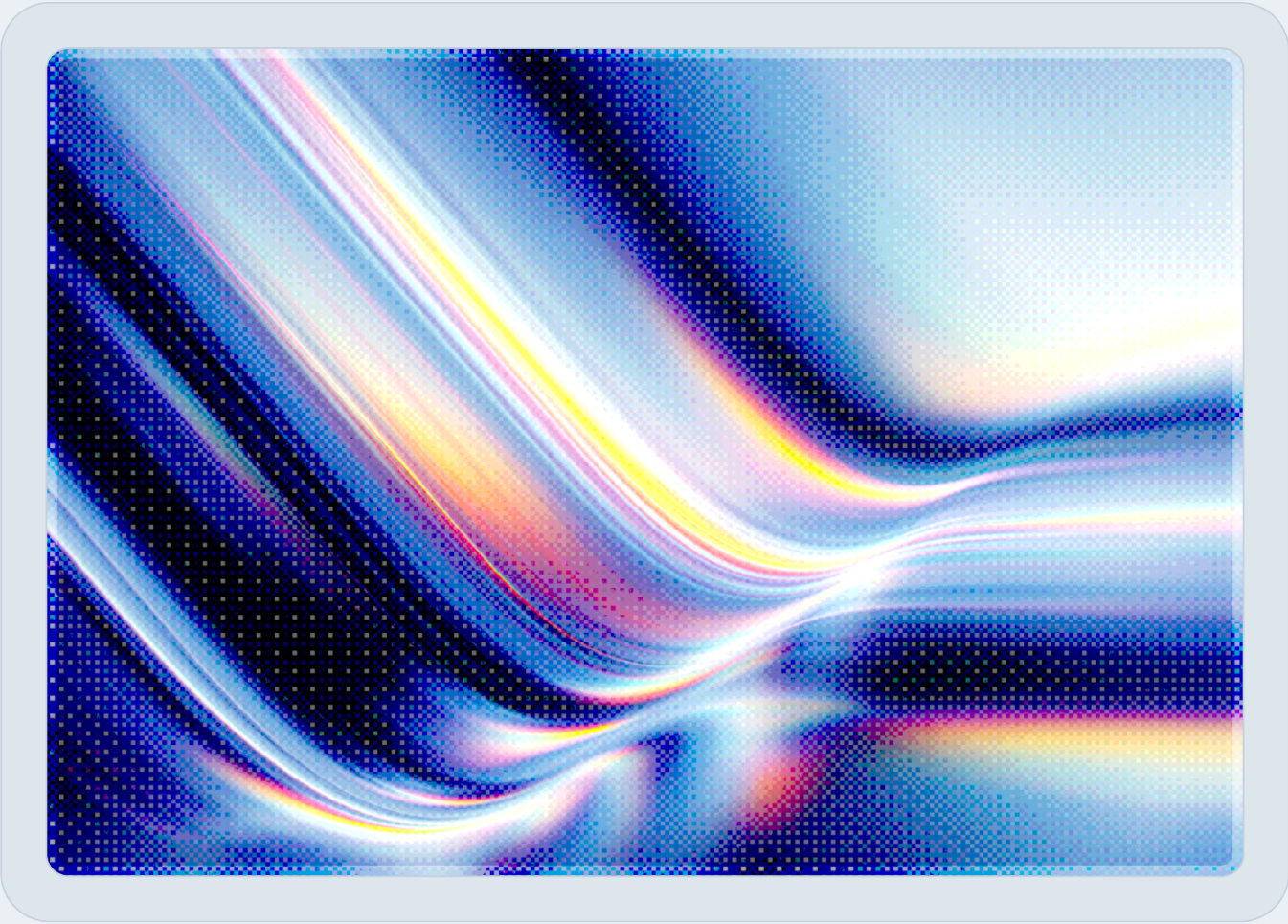
CSAI Foundation | Cloud Security Alliance

SharePoint Zero-Day CVE-2026-58644 Joins CISA KEV Under 3-Day Mandate

2026-07-17

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

Key Takeaways

CISA added CVE-2026-58644, a critical unauthenticated remote-code-execution flaw in on-premises Microsoft SharePoint Server, to its Known Exploited Vulnerabilities (KEV) catalog on July 16, 2026, after confirming active exploitation within roughly 24 hours of the patch shipping [1][2]. The vulnerability carries a CVSS base score of 9.8 and stems from unsafe deserialization of untrusted data (CWE-502), allowing an attacker to send crafted network input and execute arbitrary code without credentials or user interaction [4][5]. Based on the vulnerability's characteristics — internet exposure, KEV listing, apparent exploit automation, and full technical impact — CVE-2026-58644 appears to satisfy CISA's Binding Operational Directive (BOD) 26-04 criteria for its accelerated tier, which carries a three-day remediation deadline of July 19, 2026, rather than the traditional 21-day KEV window [1][10]. CVE-2026-58644 is one of four SharePoint vulnerabilities under active exploitation in July 2026, and the broader campaign has involved attackers chaining several of these flaws to harvest Internet Information Services (IIS) machine keys — a technique that grants durable persistence even after the underlying bug is patched — though no source reviewed for this note confirms that CVE-2026-58644 specifically has been used in that chain [2][7]. Compounding the risk, SharePoint Server 2016 and SharePoint Server 2019 — two of the three affected product lines — exited Microsoft extended support on July 14, 2026, the same day the July patch batch shipped, meaning any future vulnerability discovered in those versions is unlikely to receive an official fix absent a custom support agreement [9]. Security teams operating any on-premises SharePoint deployment, whether or not they fall under federal directives, should treat July 19 as their own internal deadline given the confirmed pre-disclosure exploitation and the scale of internet-facing SharePoint infrastructure documented by Shadowserver [8][11].

Background

Microsoft's July 2026 Patch Tuesday was, by most counts, its largest on record: depending on whether Chromium and third-party component fixes are included, the release addressed somewhere between roughly 569 and 622 distinct CVEs [9]. Buried inside that volume was a cluster of on-premises SharePoint Server fixes that CISA and independent researchers quickly flagged as more urgent than routine patch-cycle maintenance. SharePoint's history suggests it has been a recurring target for both opportunistic and sophisticated actors, largely because on-premises deployments frequently sit at the center of an organization's document management and collaboration workflows while also being

exposed, directly or indirectly, to the public internet. That combination of high business criticality and internet reachability appears to have made SharePoint Server a recurring subject of CISA emergency directives in recent years, and July 2026 extended that pattern.

The specific timeline for CVE-2026-58644 illustrates how quickly the exploitation window has compressed. Microsoft shipped the fix as part of the July 14, 2026 Patch Tuesday release, initially assessing exploitation as "more likely" rather than confirmed [4]. Within roughly a day, Microsoft revised its advisory to confirm exploitation had already been observed in the wild, and CISA responded by adding the CVE to the KEV catalog on July 16 alongside two unrelated Fortinet FortiSandbox command-injection flaws, CVE-2026-25089 and CVE-2026-39808 [1][2]. This was not an isolated incident: CISA's July 14 alert had already urged SharePoint hardening in response to separate active exploitation of CVE-2026-56164, and the broader campaign traces back further still to CVE-2026-32201 (added to KEV in April 2026) and CVE-2026-45659 (added in early July 2026) [3][9][11]. In our assessment, four SharePoint CVEs under active exploitation within a single quarter, several of them chainable into a single attack sequence, represents a materially different threat picture than a single isolated zero-day.

Security Analysis

CVE-2026-58644's technical root cause is deserialization of untrusted data (CWE-502) within Microsoft Office SharePoint's server-side processing [4][5]. In practical terms, SharePoint accepts serialized object data as part of normal request handling; when that data is not properly validated before being reconstituted into live objects, an attacker who controls the serialized payload can force the server to instantiate arbitrary code paths. The CVSS 3.1 vector for the flaw — `AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H` — indicates the vulnerability is remotely exploitable over the network, requires low attacker skill, needs no prior privileges or authentication, and needs no user interaction, while granting full compromise of confidentiality, integrity, and availability on a successful hit [4][5]. That combination is what pushes the base score to 9.8 and likely makes the vulnerability attractive to automate, since an attacker does not need to phish a user, steal a session, or already hold an account on the target server.

Some early reporting on the July SharePoint campaign described exploitation as requiring at least Site Owner–level authentication [1], which conflicts with the unauthenticated CVSS vector Microsoft itself published for CVE-2026-58644. The more likely explanation is that reporting on the broader campaign is describing a chained exploitation path — one that may combine an authenticated primitive from a related CVE with the unauthenticated deserialization bug — rather than CVE-2026-58644 in isolation.

Organizations should not assume a Site Owner account is a prerequisite for exploitation of this specific CVE; the vendor-published CVSS metrics indicate otherwise, and defenders should plan mitigations around the unauthenticated, network-exploitable case.

The table below summarizes how CVE-2026-58644 fits alongside the other three SharePoint vulnerabilities implicated in the July 2026 campaign, based on CISA KEV catalog entries and vendor advisories.

CVE	CVSS	Vulnerability Type	KEV Added	FCEB Due Date
CVE-2026-58644	9.8 (Critical)	Deserialization → RCE, unauthenticated	2026-07-16	2026-07-19
CVE-2026-56164	5.3 (Medium)	Elevation of privilege, unauthenticated	2026-07-14	2026-07-17
CVE-2026-45659	Not disclosed in reviewed sources	Remote code execution, actively exploited	2026-07-01	Not disclosed in reviewed sources
CVE-2026-32201	6.5 (Medium)	Improper input validation → spoofing	2026-04-14	2026-04-28

Sources: [1][2][3][9][11]. Where a field is marked "not disclosed in reviewed sources," the underlying reporting reviewed for this note did not provide the figure.

The CVSS score for CVE-2026-56164 is a useful cautionary data point on its own: a 5.3 "medium" rating may understate its real-world risk, given reports that attackers are chaining it with other vulnerabilities in the July campaign to escalate privileges, though the sources reviewed for this note do not confirm a specific chain terminating in CVE-2026-58644's deserialization flaw [7][9]. CISA's BOD 26-04 framework scores vulnerabilities on exposure, KEV status, exploit automation, and technical impact rather than CVSS base score alone [10] — a structure that, in effect, corrects for cases like this one where a "medium" CVSS score understates real-world urgency.

Post-exploitation activity observed in this campaign centers on theft of IIS machine keys — cryptographic material SharePoint and IIS use to protect ViewState and other serialized session data [2][7]. Once an attacker exfiltrates these keys, they can forge trusted serialized payloads that the server will deserialize and execute even after the original vulnerability is patched, unless the organization also rotates the compromised keys. This is the mechanism by which a single successful exploitation event can produce durable, patch-resistant persistence, and it is the primary reason CISA's guidance for this campaign explicitly calls for artifact removal and key rotation rather than patching alone [7].

Finally, the exposure surface for this campaign includes at least 1,300 confirmed internet-exposed instances for one related CVE alone. Shadowserver's April 2026 count identified more than 1,300 internet-exposed instances still vulnerable to CVE-2026-32201 specifically; a comparable exposure population for CVE-2026-58644's affected product lines has not been independently confirmed in the sources reviewed for this note [11]. Given that CVE-2026-58644 affects the same three product lines — SharePoint Server Subscription Edition, SharePoint Server 2019, and SharePoint Enterprise Server 2016 — a comparable population of exposed, unpatched instances should be assumed until organizations confirm otherwise through their own asset inventories [5][11].

Recommendations

Immediate Actions

Organizations running any on-premises SharePoint Server should apply the July 2026 cumulative update addressing CVE-2026-58644 without waiting for a broader change window, given confirmed pre-disclosure exploitation [1][4][6]. Because IIS machine key theft is part of the observed attack chain, patching alone is insufficient: administrators should also rotate machine keys and restart IIS on affected servers, and should review AMSI (Antimalware Scan Interface) integration status, since CISA's guidance for this campaign specifically calls out AMSI as a detection control for the deserialization payloads in use [7]. Because internet exposure is one of the four BOD 26-04 scoring criteria, temporarily removing an unpatched server from direct internet exposure should reduce its risk classification under the directive's framework — organizations should confirm this interpretation against CISA's published guidance before relying on it for compliance purposes [10].

Short-Term Mitigations

Over the following two to four weeks, security teams should establish tailored logging for SharePoint and IIS processes capable of detecting deserialization exploitation attempts and anomalous machine-key usage, and should restrict access to SharePoint Central Administration to a minimal, monitored set of administrative hosts [7]. Given that SharePoint Server 2016 and 2019 exited extended support on July 14, 2026, organizations still running those versions should treat this event as a forcing function to build a migration plan toward SharePoint Server Subscription Edition or a supported cloud alternative, since neither legacy version will receive fixes for vulnerabilities discovered from this point forward [9].

Strategic Considerations

This event reinforces the broader shift CISA initiated with BOD 26-04: prioritization based on real-world exploitability and technical impact rather than CVSS score alone [10]. Organizations should incorporate the four-variable BOD 26-04 framework — internet exposure, KEV status, exploit automation, and technical impact — into their own vulnerability management tooling so that a nominally "medium" severity finding, like CVE-2026-56164 in this campaign, is not deprioritized simply because its CVSS score looks unremarkable in isolation. Reducing the population of internet-exposed, high-value assets through Zero Trust network architecture also directly narrows the set of systems that can ever trigger an accelerated remediation timeline in the first place, since exposure is one of the four scoring variables in CISA's framework.

CSA Resource Alignment

This campaign closely tracks three areas of prior CSA research: BOD 26-04's accelerated remediation tiers, the limits of CVSS-based prioritization, and the compression of exploit timelines under AI-assisted tooling.

CSA's research note, "CISA BOD 26-04: AI Threat Forces 3-Day Critical Patch Mandate," published in June 2026, anticipated exactly this scenario: a critical, internet-exploitable, KEV-listed vulnerability landing in BOD 26-04's three-day remediation tier [12]. That note documented that AI-assisted exploit generation has compressed the gap between disclosure and weaponization from months to hours in many cases, and it recommended that organizations pre-build forensic triage playbooks compatible with 72-hour deployment windows — guidance directly applicable to the CVE-2026-58644 response described above. CSA's "The AI Vulnerability Storm" extends this theme through its "Zero Day Clock"

framing of collapsing time-to-exploit and its recommendation that organizations build a dedicated VulnOps function to keep pace — a structural response this campaign's compressed timeline argues for directly [15].

CSA's "Top Concerns With Vulnerability Data" research report is similarly relevant to the CVSS-versus-real-risk tension this campaign exposes: CVE-2026-56164's "medium" 5.3 score belies its role as a chained privilege-escalation stepping stone toward broader compromise, echoing that report's broader critique that CVE and CVSS frameworks alone are insufficient signals for prioritization decisions [13].

Finally, CSA's AI Controls Matrix (AICM) v1.1, specifically its Threat and Vulnerability Management (TVM) and Application and Interface Security (AIS) domains, provides the underlying control objectives — timely patch application, vulnerability scanning, and secure configuration management — that organizations can map their SharePoint remediation program against for audit and assurance purposes [14].

References

[1] The Hacker News. "CISA Adds Exploited SharePoint RCE Zero-Day CVE-2026-58644 to KEV." The Hacker News, July 2026.

[2] CISA. "CISA Adds Three Known Exploited Vulnerabilities to Catalog." Cybersecurity and Infrastructure Security Agency, July 16, 2026.

[3] CISA. "CISA Urges SharePoint Hardening After New Exploitations." Cybersecurity and Infrastructure Security Agency, July 14, 2026.

[4] CIRCL Vulnerability-Lookup. "CVE-2026-58644." Computer Incident Response Center Luxembourg, 2026.

[5] NIST. "CVE-2026-58644 Detail." National Vulnerability Database, 2026.

[6] Microsoft Security Response Center. "CVE-2026-58644 Update Guide." Microsoft, July 2026.

[7] BleepingComputer. "CISA Warns Admins to Patch Actively Exploited SharePoint Flaws." BleepingComputer, July 2026.

[8] SecurityWeek. "CISA Urges Immediate Patching of Exploited SharePoint Vulnerabilities." SecurityWeek, July 2026.

[9] ComplianceHub.Wiki. "622 CVEs and a Three-Day Federal Deadline: Microsoft's Record July 2026 Patch Tuesday Is a Compliance Event, Not Just a Patching One." ComplianceHub.Wiki, July 2026.

[10] CISA. "BOD 26-04: Prioritizing Security Updates Based on Risk." Cybersecurity and Infrastructure Security Agency, 2026.

[11] Petri. "Over 1,300 Internet-Exposed SharePoint Servers Remain Vulnerable." Petri, April 2026.

[12] Cloud Security Alliance. "CISA BOD 26-04: AI Threat Forces 3-Day Critical Patch Mandate." CSA AI Safety Initiative, June 2026.

[13] Cloud Security Alliance. "Top Concerns With Vulnerability Data." CSA Research Report, 2025.

[14] Cloud Security Alliance. "AI Controls Matrix (AICM) v1.1." CSA, 2026.

[15] Cloud Security Alliance. "The AI Vulnerability Storm." CSA, 2026.

