CSAI Foundation

Cloud Security Alliance AI Safety Initiative

CISA KEV Alert: Fortinet, Adobe, and Microsoft Under Attack

Unofficial AI-assisted Research

2026-04-14

Key Takeaways

- On April 13, 2026, CISA added seven vulnerabilities spanning Fortinet, Adobe, and Microsoft to its Known Exploited Vulnerabilities (KEV) catalog, confirming active exploitation of each in the wild.
- The most urgent entry, CVE-2026-21643 in Fortinet FortiClient EMS, carries a CVSS score of 9.8 and enables unauthenticated remote code execution; CISA set a remediation deadline of April 16, 2026 for federal agencies—just three days from publication.
- CVE-2026-34621, an Adobe Acrobat Reader prototype pollution zero-day, had been silently exploited since at least November 2025 before its discovery on March 26, 2026, illustrating the gap between initial compromise and detection.
- Microsoft Exchange Server vulnerability CVE-2023-21529 is actively weaponized by Storm-1175, a financially motivated threat actor, to deploy Medusa ransomware against healthcare, education, and financial organizations with as little as 24 hours between initial access and ransomware deployment [9].
- Two of the seven entries—CVE-2012-1854 (14 years old) and CVE-2020-9715 (six years old)—demonstrate that legacy vulnerabilities retain operational value for attackers long after original disclosure.

Background

CISA's Known Exploited Vulnerabilities catalog, maintained under Binding Operational Directive 22-01, represents the United States government's authoritative signal that a given vulnerability has crossed from theoretical risk to confirmed, real-world threat [2]. Inclusion requires a CVE identifier, clear remediation guidance, and reliable evidence of active exploitation. Federal Civilian Executive Branch agencies must remediate KEV entries by the assigned due date; the broader security community treats new additions as an urgent indicator regardless of sector.

April 13, 2026 brought one of the more diverse single-day KEV additions in recent memory: seven vulnerabilities affecting three major vendors across endpoint management, PDF rendering, email server infrastructure, the Windows kernel subsystem, and legacy scripting components [1, 3]. The age range alone is striking—entries span from 2012 to 2026, a fourteen-year window that underscores a persistent failure mode in enterprise patch management. Organizations that treat patching as a calendar exercise rather than a risk-driven priority will find themselves represented in this list's victim pool.

The addition arrives against a backdrop of accelerating ransomware tempo. Microsoft's April 6, 2026 threat intelligence publication on Storm-1175 described a financially motivated adversary moving from initial access to ransomware deployment in as little as 24 hours, chaining together disclosed vulnerabilities across multiple products including Microsoft Exchange [9]. CISA's April 13 update reflects, in part, the observable artifact of those campaigns: exploitation evidence that is thorough enough to meet the KEV inclusion threshold across multiple CVEs simultaneously.

Security Analysis

Fortinet FortiClient EMS: Unauthenticated SQL Injection (CVE-2026-21643)

CVE-2026-21643 is a critical SQL injection vulnerability in Fortinet FortiClient Endpoint Management Server version 7.4.4, specifically in multi-tenant deployments. With a CVSS score of 9.8, the flaw was introduced when a change to the database connection layer replaced parameterized query handling with raw string interpolation, opening a pre-authentication attack surface [5]. An adversary can inject SQL statements through the `Site` header of an HTTP request to the publicly accessible `/api/v1/init_consts` endpoint—no credentials required, and no lockout mechanism limits attempt rates [4].

The practical impact extends beyond data leakage. In Fortinet's standard virtual machine image, the PostgreSQL database user runs with superuser privileges, enabling attackers to execute operating system commands via `COPY ... TO/FROM PROGRAM`. Bishop Fox's analysis confirmed arbitrary file creation on the underlying host as the `postgres` system user [5]. From there, an adversary has access to admin password hashes, API tokens, JWT secrets, and the complete inventory of all managed endpoints—hostnames, IP addresses, OS versions, serial numbers, and installed software across an organization's entire FortiClient deployment.

Active exploitation began approximately four days before public disclosure, with Defused Cyber tracking the first observed attacks around March 24, 2026 [4]. Shadowserver counted over 2,000 publicly exposed FortiClient EMS instances, with approximately 1,400 concentrated in the United States and Europe [6]. The combination of mass internet exposure, pre-authentication exploitation, and a CISA remediation deadline of April 16, 2026—just three days after the KEV addition—makes this the single most time-sensitive entry in this wave. Organizations running version 7.4.4 in multi-tenant mode must upgrade to version 7.4.5 immediately; single-site deployments are not affected by this specific vulnerability vector.

Adobe Acrobat: A Zero-Day and a Six-Year-Old Flaw (CVE-2026-34621, CVE-2020-9715)

Adobe contributes two entries to this KEV wave. CVE-2026-34621 is the more operationally concerning: a prototype pollution vulnerability in Adobe Acrobat and Reader's JavaScript engine, assigned a CVSS score of 8.6, which had been actively exploited as a zero-day since at least November 2025 before security firm EXPMON identified a suspicious PDF sample on March 26, 2026 [7]. The sample had low antivirus detection—13 of 64 engines on VirusTotal at time of discovery—suggesting the campaign operated in relative obscurity for months.

The exploit chain is technically sophisticated. Opening a malicious PDF triggers JavaScript that leverages prototype pollution to manipulate Acrobat's internal object structures and call normally restricted privileged APIs. The observed attack used `util.readFileIntoStream()` to extract files from the local filesystem and `RSS.addFeed()` to exfiltrate the stolen data to attacker-controlled servers, followed by additional JavaScript payloads to profile victims for further escalation [8]. Adobe issued an emergency patch on April 11, 2026, two days before CISA's KEV addition [13]. Affected versions are Acrobat DC and Reader DC 26.001.21367 and earlier, and Acrobat 2024 24.001.30356 and earlier; users should update to 26.001.21411 or 24.001.30362 respectively.

CVE-2020-9715, a use-after-free memory corruption flaw disclosed in 2020, rounds out the Adobe entries [14]. Memory corruption in PDF rendering engines has a long history of weaponization because PDF is a universally trusted document format that traverses email filters, web downloads, and enterprise workflows without the scrutiny applied to executables. The

2026 confirmation of active exploitation for a six-year-old vulnerability is a reminder that attackers maintain large libraries of known-good exploits and redeploy them against organizations that lag on patching.

Microsoft: Exchange, Windows Kernel, and a 14-Year-Old Relic (CVE-2023-21529, CVE-2023-36424, CVE-2025-60710, CVE-2012-1854)

Microsoft accounts for four of the seven KEV entries, reflecting both the breadth of its attack surface and the operational persistence of threat actors targeting its infrastructure.

CVE-2023-21529 in Microsoft Exchange Server is the most contextually alarming. With a CVSS score of 8.8, this deserialization of untrusted data vulnerability allows an authenticated attacker to achieve remote code execution. Microsoft's own April 2026 threat intelligence links its exploitation directly to Storm-1175, a financially motivated group deploying Medusa ransomware across healthcare, education, professional services, and financial sectors in Australia, the United Kingdom, and the United States [9]. Storm-1175 chains CVE-2023-21529 with CVE-2022-41082 for RCE, then progresses through a practiced kill chain: creating rogue administrator accounts, deploying remote monitoring and management tools, enabling RDP via firewall modifications, using Rclone and Bandizip for data exfiltration, and finally delivering Medusa ransomware through PDQ Deployer. The entire sequence can complete within 24 hours of initial access [9, 10]. CISA and the FBI previously warned in a March 2025 joint advisory that the Medusa ransomware gang had impacted over 300 critical infrastructure organizations in the United States [17].

CVE-2023-36424 affects the Windows Common Log File System Driver, a kernel component present across essentially every supported Windows version. The flaw stems from insufficient validation in the `CClfsBaseFilePersisted::WriteMetadataBlock` function: the return value of `ClfsDecodeBlock` is not checked, enabling corruption of internal CLFS data structures. A locally authenticated attacker with any access level can exploit this to escalate privileges to SYSTEM with no user interaction and low complexity. Windows CLFS driver flaws have been a recurring ransomware enablement mechanism in recent years, as they offer a reliable post-exploitation privilege escalation path that works across a wide range of Windows versions.

CVE-2025-60710 in the Host Process for Windows Tasks (taskhostw) is a link-following vulnerability, classified under CWE-59, carrying a CVSS score of 7.8 [12]. An attacker who positions a crafted symbolic link or reparse point in the appropriate location can cause taskhostw to perform privileged I/O against attacker-controlled filesystem targets, yielding SYSTEM-level effects. Windows 11 versions 24H2 and 25H2, along with Windows Server 2025, carry the highest risk. Like CVE-2023-36424, this flaw serves a post-exploitation role: it does not provide initial access but transforms a limited foothold into full system control, making it attractive to ransomware operators seeking maximum impact after gaining entry through another vector.

Finally, CVE-2012-1854—a Microsoft Visual Basic for Applications insecure library loading vulnerability originally patched under MS12-046—returns to the security conversation in 2026. The flaw is a DLL hijacking issue: VBA's untrusted search path allows a trojan DLL placed in the same working directory as an Office document to be loaded and executed with the document user's privileges. Microsoft acknowledged limited, targeted attacks at the time of original disclosure. Its reappearance in 2026 KEV tracking indicates either that attackers have found newly unpatched instances—legacy systems operating under extended support agreements or running modified Office configurations that disable VBA sandboxing—or that the technique remains viable in targeted intrusions where defenders assume 14-year-old flaws are not active risks [11].

The Temporal Pattern: Old Bugs, Real Attacks

Taken together, the seven entries span four distinct disclosure years: 2012, 2020, 2023, and 2026. This distribution carries a direct operational implication. Attack toolkits are not updated to reflect only the newest CVEs; they are maintained libraries that continue generating value against the portion of the enterprise population that lags on patching. The median time to exploitation after KEV-listed vulnerabilities became publicly known has been shortening, but the long tail of the distribution is growing: organizations that fail to patch within weeks or months provide an indefinitely exploitable population for adversaries who have already invested in weaponization.

Recommendations

Immediate Actions

Organizations with any Fortinet FortiClient EMS deployment should treat CVE-2026-21643 as a critical emergency. Verify whether version 7.4.4 is in use and whether multi-tenant mode is enabled; if both conditions are true, upgrade to version 7.4.5 before the April 16, 2026 deadline. During the window before the patch is applied, network access to the FortiClient EMS web interface should be restricted to trusted management networks and authenticated VPN sessions wherever technically feasible. Shodan fingerprinting indicates thousands of internet-facing instances; any organization with internet-accessible FortiClient EMS should treat that exposure as an active incident until patched.

All Adobe Acrobat and Reader installations should be updated to the patched versions released April 11-12, 2026. Given that CVE-2026-34621 was exploited silently for months before discovery, security teams should also review endpoint telemetry for Acrobat processes spawning outbound network connections, particularly DNS queries or HTTP requests from Reader processes that are not associated with expected cloud service endpoints. Indicators of compromise from the observed campaign involve `util.readFileIntoStream()` and `RSS.addFeed()` API calls, which may appear in endpoint detection and response telemetry or Acrobat plugin logs.

Microsoft Exchange Server administrators must prioritize the patch for CVE-2023-21529 given its direct link to active Storm-1175 ransomware campaigns. Organizations relying on Exchange for healthcare, financial, or critical infrastructure operations should treat any unpatched instance as a likely pre-compromise target.

Short-Term Mitigations

The four Microsoft Windows entries—CVE-2023-36424, CVE-2025-60710, and the legacy CVE-2012-1854—reinforce the importance of a structured patch cycle rather than reactive emergency patching alone. Organizations should confirm that November 2023 and later Patch Tuesday updates have been fully applied across their Windows estate, as CVE-2023-36424 was originally addressed in that cycle. For CVE-2025-60710, ensure that Windows 11 24H2/25H2 and Server 2025 systems have received all security updates from early 2026. For CVE-2012-1854, the primary mitigation remains applying MS12-046 and subsequent Office security updates; organizations that have not applied patches from 2012 should treat their VBA-enabled Office installations as compromised infrastructure.

Network defenders should review detection rules for Storm-1175 TTPs, including creation of new administrator accounts, anomalous RMM tool installations (particularly PDQ Deployer), Rclone or Bandizip execution, and large outbound data transfers. Detection opportunities exist at each stage of the kill chain before ransomware deployment.

Strategic Considerations

This KEV wave is diagnostic of a structural vulnerability management failure that affects organizations across sectors. Seven actively exploited vulnerabilities spanning 14 years of disclosure history means that attackers are finding a sufficient population of unpatched targets to justify operating exploit code that dates to 2012. Organizations should assess whether their vulnerability management programs are genuinely risk-driven—prioritizing by exploitation evidence and asset criticality—or whether they operate on fixed-cadence cycles that create predictable exploitation windows.

Vulnerability management tooling should be integrated with KEV catalog feeds. CISA publishes the catalog in machine-readable JSON format at `https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json`, enabling automated correlation between internal asset inventories and actively exploited vulnerabilities. Organizations that cannot determine within hours whether a newly KEV-listed product version is present in their environment have an asset inventory gap that predates and exceeds any individual vulnerability.

The Storm-1175 pattern—24-hour ransomware deployment from initial access—argues against treating Exchange patching as a planned maintenance activity. When adversaries are operating at that tempo, a three-week patch cycle that begins after the next change-control board meeting represents an unacceptable exposure window. Organizations with internet-facing Exchange should evaluate emergency patching procedures and consider temporary access restriction through application gateway or VPN-gating of Exchange ports during the period before patches are applied.

CSA Resource Alignment

The vulnerabilities catalogued in this KEV wave intersect with multiple CSA frameworks and guidance materials, each of which provides structured control language for organizations working to operationalize their response.

The CSA Cloud Controls Matrix (CCM), currently at version 4.0, includes the Threat and Vulnerability Management (TVM) domain, which embeds risk-based remediation practices and maps to ISO 27001, NIST SP 800-53, and PCI DSS [15]. TVM controls directly govern the processes that determine how quickly an organization identifies and remediates exploitable vulnerabilities in cloud-hosted or cloud-adjacent infrastructure such as Exchange Online hybrid environments and cloud-delivered FortiClient EMS. Organizations seeking to benchmark their patch management practices against an internationally recognized framework should map their current remediation SLAs to the CCM TVM control objectives.

The AI Controls Matrix (AICM), CSA's extension of the CCM for AI-specific risks, is relevant here in a second-order sense: organizations deploying AI-powered security operations tooling (such as AI-assisted SIEM analysis or AI-driven vulnerability correlation) that relies on document ingestion—including PDF parsing—face compounded risk from CVE-2026-34621. A malicious PDF that exploits the Acrobat prototype pollution flaw could potentially be routed through AI document pipelines, exfiltrating data from AI processing environments. The AICM's data security and supply chain control domains address these risk intersections [16].

CSA's Zero Trust guidance is directly applicable to the lateral movement and privilege escalation patterns observed in this wave. Storm-1175's reliance on compromised administrator credentials and living-off-the-land techniques—both of which succeed because internal network segments implicitly trust authenticated principals—is precisely the adversary pattern that a

zero trust architecture defeats by requiring continuous verification and least-privilege enforcement at every access decision. Organizations evaluating their exposure to Exchange-based initial access followed by credential-based lateral movement should use CSA's Zero Trust publications as a reference architecture for reducing that exposure surface.

The CISA KEV catalog itself aligns with CSA STAR (Security, Trust, Assurance, and Risk) program expectations, which require cloud service providers to demonstrate structured vulnerability management and patch compliance processes. STAR-registered organizations that consume Fortinet or Adobe products as part of their cloud service delivery should document how this KEV wave was processed within their vulnerability management lifecycle as part of ongoing STAR continuous monitoring obligations.

References

[1] CISA. "CISA Adds Seven Known Exploited Vulnerabilities to Catalog." CISA, April 13, 2026.

[2] CISA. "BOD 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities." CISA, November 2021.

[3] SecurityAffairs. "U.S. CISA adds Adobe, Fortinet, Microsoft Exchange Server, and Microsoft Windows flaws to its Known Exploited Vulnerabilities catalog." SecurityAffairs, April 14, 2026.

[4] Help Net Security. "Critical Fortinet FortiClient EMS bug under active attack (CVE-2026-21643)." Help Net Security, March 30, 2026.

[5] Bishop Fox. "Pre-Authentication SQL Injection in FortiClient EMS 7.4.4." Bishop Fox, 2026.

[6] BleepingComputer. "Critical Fortinet FortiClient EMS flaw now exploited in attacks." BleepingComputer, 2026.

[7] SecurityAffairs. "Adobe fixes actively exploited Acrobat Reader flaw CVE-2026-34621." SecurityAffairs, April 2026.

[8] Help Net Security. "Adobe issues emergency fix for Acrobat Reader flaw exploited in the wild (CVE-2026-34621)." Help Net Security, April 13, 2026.

[9] Microsoft Security Blog. "Storm-1175 focuses gaze on vulnerable web-facing assets in high-tempo Medusa ransomware operations." Microsoft, April 6, 2026.

[10] Dark Reading. "Storm-1175 Deploys Medusa Ransomware at 'High Velocity'." Dark Reading, 2026.

[11] The Register. "Zombie Microsoft bugs rise from the dead, pave way for crims and ransomware scum." The Register, April 13, 2026.

[12] Microsoft MSRC. "CVE-2025-60710: Host Process for Windows Tasks Elevation of Privilege Vulnerability." Microsoft, 2026.

[13] NVD. "CVE-2026-34621 Detail." NIST National Vulnerability Database, 2026.

[14] Tenable. "CVE-2020-9715." Tenable, 2026.

[15] CSA. "Cloud Controls Matrix v4.0." Cloud Security Alliance, 2025.

[16] CSA. "AI Controls Matrix." Cloud Security Alliance, 2025.

[17] CISA and FBI. "#StopRansomware: Medusa Ransomware." CISA Advisory AA25-071a, March 2025.

