INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-15 09:16 UTC

Microsoft SharePoint Server - Microsoft SharePoint Server Improper Input Validation Vulnerability

CVE VULNERABILITY | **HIGH** | CVSS 7.5 | **CISA KEV**

SCC Item ID	SCC-CVE-2026-0041
Type	CVE Vulnerability
CVE ID	CVE-2026-32201
Severity	HIGH
CVSS Base Score	7.5
KEV Status	Yes — CISA Known Exploited Vulnerability (due: 2026-04-28)
Affected Products	Microsoft SharePoint Server
Published	2026-04-14
Discovery Source	Cisa Kev

Executive Summary

A confirmed, actively exploited vulnerability in Microsoft SharePoint Server allows remote attackers to perform spoofing attacks without authentication, compromising the integrity of identity and content workflows. CISA has added this to its Known Exploited Vulnerabilities catalog with a remediation deadline of April 28, 2026, indicating confirmed exploitation in the wild. Organizations running SharePoint Server face immediate risk of unauthorized access, credential abuse, and potential lateral movement across enterprise collaboration infrastructure.

Technical Analysis

CVE-2026-32201 is an improper input validation vulnerability (CWE-20) in Microsoft SharePoint Server with a CVSS base score of 7.5 (High). The flaw enables an unauthenticated remote attacker to conduct spoofing attacks over the network, without requiring user interaction or elevated privileges at the point of entry. Mapped MITRE ATT&CK techniques include T1078 (Valid Accounts), T1566 (Phishing), and T1199 (Trusted Relationship), suggesting exploitation pathways that abuse authentication trust boundaries or manipulate input to impersonate legitimate users or services. The vulnerability was disclosed as part of Microsoft's April 2026 Patch Tuesday (163 CVEs addressed), with details available in the Microsoft Security Response Center advisory at https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-32201. CISA confirmed

active exploitation and set a federal remediation due date of 2026-04-28. Specific affected SharePoint Server versions and patch IDs are published in the MSRC advisory. EPSS data was not available at time of publication; prioritize remediation based on CISA KEV status alone.

Action Checklist

1. Step 1: Containment. Identify all SharePoint Server instances in your environment immediately. Restrict external network access to SharePoint Server at the perimeter firewall or WAF if patching cannot begin immediately. A 24-hour containment window is recommended as a baseline, but adjust based on your organization's risk tolerance and operational capacity. Review the Microsoft MSRC advisory (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-32201) to confirm affected versions against your inventory.
2. Step 2: Detection. Review SharePoint ULS logs and Windows Security Event logs for anomalous authentication events, unexpected account activity (Event IDs 4624, 4625, 4648), and spoofed or malformed HTTP requests to SharePoint endpoints. Query SIEM for T1078 indicators: logins from unusual source IPs, off-hours access, or accounts accessing SharePoint resources outside normal behavioral baselines. Check for T1199 indicators: unexpected trusted-relationship or service account activity against SharePoint.
3. Step 3: Eradication. Apply the patch released in Microsoft's April 2026 Patch Tuesday update cycle. Obtain the specific KB article and patch ID from the MSRC advisory (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-32201). Follow Microsoft's documented update path for your SharePoint Server version. Do not defer past the CISA KEV due date of 2026-04-28.
4. Step 4: Recovery. After patching, verify patch installation via Windows Update history or deployment management tooling. Audit SharePoint access logs for the period between initial disclosure and patch application. Reset credentials for any service accounts or user accounts showing anomalous SharePoint activity. Validate that no unauthorized sharing permissions, app registrations, or external access links were created during the exposure window.
5. Step 5: Post-Incident. Review input validation controls and WAF rule coverage for SharePoint-facing endpoints. Assess whether SharePoint Server instances are unnecessarily internet-facing and scope reduction is feasible. Evaluate whether privileged SharePoint service accounts follow least-privilege principles. Document gap between patch release and deployment completion; use this to improve patch SLA for CISA KEV-listed vulnerabilities going forward.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO, legal counsel, and breach notification assessment if forensic review of SharePoint audit logs or IIS access logs reveals successful spoofed-identity authentication (Event ID 4624 with Logon Type 3 from external IPs, or SharePoint audit entries showing 'SecRoleBindUpdate' or 'AppInstalled' events from unexpected accounts) during the exposure window, particularly where the affected SharePoint instance hosts PII, PHI, financial records, or content subject to HIPAA, PCI-DSS, or state breach notification statutes.

Recovery Notes	After patching, monitor SharePoint ULS logs and Windows Security Event logs continuously for a minimum of 30 days for recurrence of anomalous authentication patterns (Event IDs 4624/4648 from external IPs, unexpected service account logons) that may indicate a threat actor established persistent access prior to containment. Verify that all SharePoint application pool identities, farm service accounts, and site collection administrator lists match your pre-incident baseline, and re-run the permission audit ('Get-SPAuditEntry' filtered on 'SecRoleBindUpdate') weekly for 30 days to detect any delayed activation of unauthorized grants created during the exposure window. If the affected SharePoint instance was internet-facing during the exposure window and hosted sensitive content, initiate a formal data exposure assessment to determine whether breach notification obligations under applicable regulations are triggered.
Forensic Artifacts	IIS W3C access logs at '%SystemDrive%\inetpub\logs\LogFiles\W3SVC*' — filter for requests to SharePoint authentication endpoints ('/_windows/default.aspx', '/_trust/', '/_vti_bin/SecurityTokenServiceApplication/') with anomalous or malformed Authorization headers, unexpected HTTP verb usage, or source IPs not present in normal user traffic baselines, which would indicate CVE-2026-32201 exploit attempts targeting the improper input validation flaw. | SharePoint ULS logs at 'C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\16\LOGS\' — filter on Category 'Authentication Authorization' and 'Claims Authentication' for entries reflecting identity claims that bypassed normal validation, spoofed UPN or SID values, or authentication failures followed immediately by successes from the same source, consistent with an improper input validation spoofing attack. | Windows Security Event Log entries for Event ID 4648 (A logon was attempted using explicit credentials) and Event ID 4624 (Logon Type 3, Network) attributed to SharePoint application pool service accounts (spfarm, spservices) or unknown accounts accessing SharePoint resources — these events would surface when a spoofed identity is used to authenticate to SharePoint-integrated services or downstream systems after exploitation. | SharePoint content database audit log entries queryable via 'Get-SPSite | Get-SPAuditEntry' filtered on event types 'SecRoleBindUpdate' (permission changes), 'SecRoleBindBreakInheritance' (inheritance breaks indicating attempted privilege establishment), and 'AppInstalled' (unauthorized app registrations) — these artifact types reflect post-exploitation persistence and access expansion actions a spoofing attacker would perform after successfully bypassing SharePoint identity validation. | Pre- and post-patch SHA-256 file hashes of 'Microsoft.SharePoint.dll' at 'C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\16\ISAPI\Microsoft.SharePoint.dll' — the vulnerable DLL is the component responsible for input validation in SharePoint's authentication pipeline, and hash comparison confirms whether the vulnerable binary was replaced by the April 2026 Patch Tuesday cumulative update targeting CVE-2026-32201.

Per-Action IR Details

Step 1: Containment — Identify all SharePoint Server instances in your environment immediately. Restrict external network access to SharePoint Server at the perimeter firewall or WAF if patching cannot begin within 24 hours. Review the Microsoft MSRC advisory (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-32201) to confirm affected versions against your inventory.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Run 'Get-SPFarm | Get-SPServer' on each candidate SharePoint host to enumerate farm members; cross-reference against DNS and firewall rule exports. Block TCP 443 and TCP 80 inbound to SharePoint front-end servers at the host firewall using 'netsh advfirewall firewall add rule name="Block-SPExternal" dir=in action=block protocol=tcp localport=80,443 remoteip=0.0.0.0/0' as an emergency stop-gap. For WAF-less environments, deploy a free reverse-proxy ACL via nginx with 'deny all' on the upstream SharePoint location block to restrict external IPs while maintaining internal access.

Evidence: Before isolating, capture a full snapshot of active SharePoint IIS site bindings ('Get-WebBinding -Name "SharePoint*"' via PowerShell), current IIS worker process list ('Get-Process w3wp'), and netstat output ('netstat -ano | findstr :443') to document all active sessions to SharePoint endpoints at time of containment. Preserve the IIS access logs at '%SystemDrive%\inetpub\logs\LogFiles\W3SVC*' without modification — these will be the primary source for pre-containment exploit attempts.

Step 2: Detection — Review SharePoint ULS logs and Windows Security Event logs for anomalous authentication events, unexpected account activity (Event IDs 4624, 4625, 4648), and spoofed or malformed HTTP requests to SharePoint endpoints. Query SIEM for T1078 indicators: logins from unusual source IPs, off-hours access, or accounts accessing SharePoint resources outside normal behavioral baselines. Check for T1199 indicators: unexpected trusted-relationship or service account activity against SharePoint.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-2 (Event Logging), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, parse SharePoint ULS logs directly: ULS logs are located at 'C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\16\LOGS\' and can be filtered with the ULS Viewer tool (free, Microsoft-provided) — filter on Category 'Authentication Authorization' and Severity 'High' or 'Critical'. For Windows Security Event Log, run: 'Get-WinEvent -LogName Security | Where-Object {$_.Id -in 4624,4625,4648} | Where-Object {$_.Message -match "SharePoint|spfarm|svc_sp"} | Export-Csv sp_auth_events.csv' to isolate SharePoint service account and spoofed-identity events. Deploy the free Sigma rule for T1078 (Valid Accounts) from the SigmaHQ repository against Windows Security logs using sigma-cli with an evtx backend to generate PowerShell-compatible queries without a SIEM.

Evidence: Capture the SharePoint ULS log files at 'C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\16\LOGS\' covering the full exposure window (from initial MSRC disclosure date through containment). Preserve IIS W3C access logs for all SharePoint web application pools, specifically filtering for HTTP requests containing malformed or unexpected 'Authorization' headers, unusual user-agent strings, and requests to SharePoint authentication endpoints ('/_windows/default.aspx', '/_trust/', '/SecurityTokenServiceApplication/'). Extract Windows Security Event Log entries for Event ID 4648 (explicit credential logon) originating from the SharePoint application pool service account identity, as spoofing attacks against SharePoint authentication may surface as the service account presenting credentials on behalf of a forged identity.

Step 3: Eradication — Apply the patch released in Microsoft's April 2026 Patch Tuesday update cycle. Obtain the specific KB article and patch ID from the MSRC advisory (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-32201). Follow Microsoft's documented update path for your SharePoint Server version. Do not defer past the CISA KEV due date of 2026-04-28.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CM-3 (Configuration Change Control), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For environments without WSUS or SCCM, download the SharePoint cumulative update KB directly from the Microsoft Update Catalog (catalog.update.microsoft.com) and deploy via the SharePoint Products Configuration Wizard with 'psconfig.exe -cmd upgrade -inplace b2b -wait -force' run on all farm servers in the correct

sequence (database server first, then application servers, then front-end web servers). Verify patch application by querying the farm build version: 'Get-SPFarm | Select BuildVersion' — the post-patch build number must match the version documented in the April 2026 CU release notes from the MSRC advisory. Script this check across all farm members with 'foreach ($s in (Get-SPServer)) { Invoke-Command -ComputerName $s.Name -ScriptBlock { (Get-SPFarm).BuildVersion } }'.

Evidence: Before applying the patch, capture a binary hash of the SharePoint core DLLs affected by the improper input validation flaw (specifically 'Microsoft.SharePoint.dll' located at 'C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\16\ISAPI\') using 'Get-FileHash -Algorithm SHA256' to establish a pre-patch baseline. This pre-patch hash documents the vulnerable binary state and can later confirm that the patched DLL replaced the vulnerable version. Also capture the current SharePoint farm build version via 'Get-SPFarm | Select BuildVersion' as a pre-patch benchmark.

Step 4: Recovery — After patching, verify patch installation via Windows Update history or deployment management tooling. Audit SharePoint access logs for the period between initial disclosure and patch application. Reset credentials for any service accounts or user accounts showing anomalous SharePoint activity. Validate that no unauthorized sharing permissions, app registrations, or external access links were created during the exposure window.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST AU-11 (Audit Record Retention), NIST IA-5 (Authenticator Management), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Audit SharePoint sharing permissions and external access links without commercial tooling by running 'Get-SPSite -Limit ALL | Get-SPWeb -Limit ALL | foreach { $_.Lists | foreach { $_.RoleAssignments } }' to enumerate all non-inherited permission grants created during the exposure window — filter results by date of creation matching the disclosure-to-patch window. To enumerate app registrations added during the exposure window, query SharePoint's App Management Service database or use 'Get-SPAppInstance -Web ' across all site collections. Perform credential resets for SharePoint service accounts (spfarm, spservices, spprofile, spsearch) via Active Directory 'Set-ADAccountPassword' and immediately cycle the application pool identity passwords in IIS Manager on all front-end servers.

Evidence: Collect and preserve the SharePoint audit log database entries (stored in each site collection's content database, queryable via 'Get-SPSite | Get-SPAuditEntry') for the full exposure window, filtering on audit event types 'SecRoleBindUpdate', 'SecRoleBindBreakInheritance', and 'AppInstalled' — these event types would reflect unauthorized permission grants or app registrations that a spoofing attacker may have created. Also export the SharePoint site collection administrator list ('Get-SPSite | Select Url, SecondaryContact, @{N="SiteAdmins";E={$_.RootWeb.SiteAdministrators}}') as a baseline to identify any admin-level accounts added during the exposure window.

Step 5: Post-Incident — Review input validation controls and WAF rule coverage for SharePoint-facing endpoints. Assess whether SharePoint Server instances are unnecessarily internet-facing and scope reduction is feasible. Evaluate whether privileged SharePoint service accounts follow least-privilege principles. Document gap between patch release and deployment completion; use this to improve patch SLA for CISA KEV-listed vulnerabilities going forward.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-10 (Information Input Validation), NIST RA-3 (Risk Assessment), NIST AC-6 (Least Privilege), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For WAF rule coverage review without a commercial WAF, deploy OWASP ModSecurity CRS rules (free, open source) targeting SharePoint authentication endpoints — specifically add rules blocking requests with

malformed 'Authorization' header values and unexpected SOAP action strings targeting SharePoint's Security Token Service ('/_vti_bin/SecurityTokenServiceApplication/'). Enumerate SharePoint service account privileges in Active Directory by running 'Get-ADUser -Filter {ServicePrincipalName -like "*sharepoint*"} | Get-ADUser -Properties MemberOf | Select Name, MemberOf' to identify any service accounts with Domain Admin or excessive group membership that should be scoped down. Document the patch deployment gap in a formal lessons-learned memo referencing the CISA KEV deadline of 2026-04-28 and the actual deployment completion date to quantify SLA breach, if any.

Evidence: Compile the final forensic timeline from IIS access logs, ULS logs, Windows Security Event logs (Event IDs 4624, 4625, 4648), and SharePoint audit log entries spanning from the earliest suspicious request through patch verification, to document whether exploitation occurred during the exposure window. Retain all collected log archives and memory/disk images (if acquired) per your organization's incident record retention schedule in alignment with NIST AU-11 (Audit Record Retention) — minimum 1 year for most regulatory environments, longer if PII or regulated data was accessible via the affected SharePoint instance.

Detection Guidance

Focus detection on authentication anomalies and input manipulation patterns targeting SharePoint Server. Key sources: SharePoint ULS logs, IIS access logs for the SharePoint web application, and Windows Security Event logs on SharePoint servers. Look for: malformed or unexpected input in HTTP POST requests to SharePoint endpoints (/_api/, /_layouts/, /sites/); authentication events where the claimed identity does not match source IP or session context (Event IDs 4624 type 3 with unusual sources, 4648); service account logins outside scheduled or expected patterns (T1078/T1199); and repeated 400/401/403 responses that could indicate probing. In your SIEM, build a detection rule correlating SharePoint IIS 401 responses followed by successful 200 responses from the same source IP within a short window - this pattern may indicate spoofing success after initial rejection. Cross-reference with MITRE ATT&CK T1566 indicators if phishing-delivered payloads are suspected as an initial access vector feeding into SharePoint exploitation.

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1566** — Phishing
- **T1199** — Trusted Relationship

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring

- **SI-8** — Spam Protection
- **SI-10** — Information Input Validation
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A03:2021** — Injection

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

ISO-27001-2022

- **A.8.26** — Application security requirements
- **A.8.8** — Management of technical vulnerabilities

NIST-CSF-2

- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1566	Phishing	Initial-Access
T1199	Trusted Relationship	Initial-Access

Sources

Source	URL	Tier
cisa_kev	https://www.cisa.gov/known-exploited-vulnerabilities-catalog	T1
CVE-2026-32201 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-32201	T1
CVE-2026-32201 - CVE Record	https://www.cve.org/CVERecord?id=CVE-2026-32201	T3
Security Update Guide - Microsoft Security Response Center	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-202...	T1

Source	URL	Tier
Microsoft's April 2026 Patch Tuesday Addresses 163 CVEs (CVE ...	https://www.tenable.com/blog/microsofts-april-2026-patch-tuesday-ad...	T3
Microsoft Security Advisory	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-32201	T1

Generated 2026-04-15 09:16 UTC by TJS Security Command Center