INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:38 UTC

ToolShell: Active Exploitation of Critical Microsoft SharePoint Vulnerability Chain

THREAT CAMPAIGN | CRITICAL

SCC Item ID	SCC-CAM-2026-0041
Type	Threat Campaign
Severity	CRITICAL
Affected Products	Microsoft SharePoint Server (on-premises); specific versions not confirmed from available data, see Microsoft Security Blog for version scope
Published	2026-03-19

Executive Summary

Microsoft's on-premises SharePoint Server is under active exploitation via a multi-stage attack chain Microsoft has named ToolShell, targeting a critical vulnerability patched in January 2025. Organizations running on-premises SharePoint that have not applied the January 2025 security updates are at immediate risk of compromise. Successful exploitation can give attackers a foothold inside the corporate network, with potential for data exfiltration, lateral movement, and broader infrastructure compromise.

Technical Analysis

ToolShell is a multi-stage exploit chain targeting on-premises Microsoft SharePoint Server, exploiting a critical vulnerability addressed in Microsoft's January 2025 Patch Tuesday release. The primary MITRE technique is T1190 (Exploit Public-Facing Application). Microsoft confirmed active exploitation in July 2025 and published disruption guidance; CISA has also confirmed in-the-wild exploitation. Cyberbit has published campaign-specific technical analysis of the exploit chain stages. CVE identifier was not confirmed in available source metadata and is not fabricated here, consult the Microsoft Security Blog (https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/) for the authoritative CVE reference and affected version matrix. CWE classification is not confirmed from available data. CVSS and EPSS scores were not present in the source data; treat severity as critical based on Microsoft and CISA designations. The vulnerability is specific to on-premises deployments; SharePoint Online (Microsoft 365) is not reported as affected.

Action Checklist

1. Step 1, Patch immediately: Apply Microsoft's January 2025 Patch Tuesday SharePoint security updates to all on-premises SharePoint Server instances. Verify patch status against the affected version list in the Microsoft Security Blog before marking systems as remediated.
2. Step 2, Hunt for compromise indicators: Review SharePoint server logs, IIS logs, and Windows Event Logs for anomalous HTTP requests, unexpected process spawning from SharePoint worker processes (w3wp.exe), and unusual outbound connections from SharePoint hosts. Reference Cyberbit's ToolShell campaign analysis for stage-specific behavioral indicators.
3. Step 3, Inventory exposure: Identify all on-premises SharePoint Server instances across the environment, including dev, staging, and legacy systems. Confirm whether any are internet-facing and prioritize those for immediate patching and investigation.
4. Step 4, Notify stakeholders: Alert leadership and relevant business unit owners if SharePoint is used for sensitive data or critical workflows. If indicators of compromise are found, initiate incident response procedures and escalate accordingly.
5. Step 5, Review compensating controls and architecture: Assess whether on-premises SharePoint instances require direct internet exposure. Where possible, restrict access via VPN or zero-trust network controls. Review web application firewall rules for SharePoint-specific coverage and evaluate migration timelines to SharePoint Online where operationally viable.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and external IR firm immediately if hunt in Step 2 uncovers process spawning from w3wp.exe, unexpected outbound connections to non-corporate networks, or file modifications in SharePoint directories post-exploitation timeframe.
Recovery Notes	Post-eradication: validate all SharePoint Server instances are patched and baseline event logging is re-enabled. Conduct full credential reset for service accounts running SharePoint pools (reset at-rest passwords and rotation schedules). Restore SharePoint content from verified clean backups (dated pre-exploitation) and validate no malicious custom solutions or web parts remain in solution store via 'Get-SPSolution | Select-Object Name, SolutionId, Deployed'. Document recovery timeline and affected data scope per NIST 800-61r3 §3.4.
Forensic Artifacts	IIS HTTP Request Logs (C:\inetpub\logs\LogFiles\W3SVC**.log) — POST requests to /_vti_bin/, suspicious QueryStrings, 200/302 responses | Windows Security Event Log (Event ID 4688, 4689, 4624, 4625) — process creation from w3wp.exe, authentication failures, account lockouts | SharePoint ULS Logs (C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\[version]\LOGS\) — custom code execution, timer job anomalies, user profile service events | w3wp.exe Memory Dump (ProcDump -ma w3wp.exe) — injected code, shellcode patterns, suspicious DLL loads | Network Traffic Captures (tcpdump, netsh trace, proxy logs) — outbound connections from SharePoint host to external IPs, DNS queries to suspicious domains

Per-Action IR Details

Step 1 — Patch immediately: Apply Microsoft's January 2025 SharePoint security updates to all on-premises SharePoint Server instances. Verify patch status against the affected version list in the Microsoft Security Blog before marking systems as remediated.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation Phase)

Controls: NIST 800-53 SI-2 (Flaw Remediation), CIS 4.7 (Update Operating Systems), CIS 16.11 (Patch Management)

Compensating: For air-gapped environments: obtain Microsoft patches via WSUS offline sync or direct download to isolated media; validate checksums against Microsoft Security Update Guide before deployment. Use 'Get-SPProduct -Local' PowerShell cmdlet to confirm pre- and post-patch version numbers. Stagger deployment across non-production instances first to validate compatibility.

Evidence: Capture baseline system snapshots (file hashes of SharePoint binaries, registry keys HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall) BEFORE patching. Document current patch levels with 'Get-HotFix' output and SharePoint version via 'Get-SPFarm' cmdlet. This creates a forensic record of pre-patch state.

Step 2 — Hunt for compromise indicators: Review SharePoint server logs, IIS logs, and Windows Event Logs for anomalous HTTP requests, unexpected process spawning from SharePoint worker processes (w3wp.exe), and unusual outbound connections from SharePoint hosts. Reference Cyberbit's ToolShell campaign analysis for stage-specific behavioral indicators.

NIST Phase: Detection Analysis

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

Controls: NIST 800-53 AU-2 (Audit Events), NIST 800-53 SI-4 (Information System Monitoring), CIS 8.1 (Establish Centralized Log Management), CIS 13.7 (Verify User Activity)

Compensating: Without SIEM: parse logs locally using PowerShell or grep. Check IIS logs (C:\inetpub\logs\LogFiles\W3SVC**.log) for POST requests to /_vti_bin/ or /sites/ with unusual QueryStrings; grep for HTTP 200/302 responses to suspicious payloads. Check Windows Event Viewer for Event ID 4688 (Process Creation) filtering for w3wp.exe spawning cmd.exe, powershell.exe, or rundll32.exe. Use 'Get-EventLog -LogName Security -InstanceId 4688 -ComputerName [hostname] | Where-Object {$_.Message -match 'w3wp'}'.

Evidence: Preserve unmodified IIS logs (entire W3SVC* directories), Windows Security Event Log exports (Event IDs 4688, 4689, 4624, 4625), and application event logs for SharePoint. Capture memory dump of w3wp.exe processes (use ProcDump.exe -ma w3wp.exe for forensic analysis) and network traffic via netsh trace if available. Extract SharePoint ULS logs (C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\[version]\LOGS\) before analysis.

Step 3 — Inventory exposure: Identify all on-premises SharePoint Server instances across the environment, including dev, staging, and legacy systems. Confirm whether any are internet-facing and prioritize those for immediate patching and investigation.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation Phase - Tools and Resources)

Controls: NIST 800-53 CM-8 (Information System Component Inventory), CIS 1.1 (Establish Information and Resource Management), CIS 2.1 (Maintain Inventory of Network Assets)

Compensating: Use native tools: 'nslookup' and 'nmap -p 443,80' against domain suffixes (e.g., sharepoint.company.com) to identify public DNS records. Query Active Directory via PowerShell: 'Get-ADComputer -Filter {Name -like "*sharepoint*"} -Properties *'. Cross-reference with firewall rules using 'netsh advfirewall show rule name=all | grep -i sharepoint'. For legacy systems, check DHCP logs and network device configurations. Document in spreadsheet with columns: Hostname | IP | Version | Internet-Facing (Y/N) | Patch Level | Owner.

Evidence: Export network discovery scan results (nmap XML output), Active Directory computer objects with DNS registration timestamps, firewall rule exports, and network flow logs showing inbound traffic to SharePoint ports (443, 80, 32843). Preserve DHCP server logs showing lease assignments to SharePoint hosts.

Step 4 — Notify stakeholders: Alert leadership and relevant business unit owners if SharePoint is used for sensitive data or critical workflows. If indicators of compromise are found, initiate incident response procedures and escalate accordingly.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.4 (Incident Notification)

Controls: NIST 800-53 IR-1 (Incident Response Policy), NIST 800-53 IR-6 (Incident Reporting), CIS 19.1 (Establish an Incident Response Process)

Compensating: Without formal IR team: use pre-established escalation contacts (document in runbook). Draft notification using NIST 800-61r3 template: include affected systems, compromise indicators found (specific), potential data exposure scope, immediate containment actions taken, and recommended next steps. Send via secure channel (encrypted email or in-person). Document time/recipient/content in incident log. Activate incident response team checklist per your organization's IR plan.

Evidence: Capture all evidence files referenced in Steps 2-3 (IIS logs, event logs, network traffic, ULS logs) before notifying stakeholders. Secure chain of custody for evidence: document who collected what, when, and on what media. This prevents stakeholder pressure to share incomplete findings. Document notification times and recipients in incident timeline.

Step 5 — Review compensating controls and architecture: Assess whether on-premises SharePoint instances require direct internet exposure. Where possible, restrict access via VPN or zero-trust network controls. Review web application firewall rules for SharePoint-specific coverage and evaluate migration timelines to SharePoint Online where operationally viable.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 (Containment, Eradication, and Recovery)

Controls: NIST 800-53 AC-2 (Account Management), NIST 800-53 AC-3 (Access Enforcement), NIST 800-53 SC-7 (Boundary Protection), CIS 12.3 (Address Unauthorized Software), CIS 14.1 (Establish Secure Configuration Management)

Compensating: No WAF: configure firewall rules blocking direct inbound HTTP(S) to SharePoint; require VPN or proxy access. Test via: 'nmap -p 443 [sharepoint-external-ip]' (should return filtered/closed after rule deployment). For zero-trust simulation: implement IP allowlist for known subnets; log all connection attempts to syslog for review. Use SharePoint's built-in IP restrictions: Central Admin > Manage Web Applications > Authentication Providers > Edit Zone > IP Allow List. Document baseline firewall rules (export via netsh or vendor CLI) before changes; maintain rollback procedure.

Evidence: Preserve baseline network topology diagrams, current firewall rules (vendor-specific exports), SharePoint architecture documentation (site collections, web applications, zones). Capture network traffic flow data showing current inbound sources to SharePoint. If migration to Online is planned, document current on-premises authentication scheme (ADFS, Kerberos) and content migration scope for forensic reference if compromise occurred pre-migration.

Detection Guidance

Focus detection efforts on the SharePoint server itself and downstream network activity. Key areas to examine: (1) IIS logs on SharePoint servers, look for unusual POST requests to SharePoint application endpoints, particularly those involving /_layouts/ or /_api/ paths with anomalous parameters or payloads. (2) Windows Event Logs, monitor for process creation events (Event ID 4688) where parent process is w3wp.exe or SharePoint-related services spawning cmd.exe, powershell.exe, or other shell processes. (3) Outbound network connections, flag unexpected outbound connections from SharePoint hosts to external IPs, particularly on non-standard ports. (4) File system changes, monitor for new files written to SharePoint web directories or system directories by IIS worker processes. Consult the Microsoft Security Blog disruption guidance (July 2025) and Cyberbit's ToolShell campaign page for campaign-specific indicators. CISA's Known Exploited Vulnerabilities catalog should be checked for any published IOCs associated with this campaign. No specific IOCs (IPs, hashes, domains) were present in the available source metadata and are not fabricated here.

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application

NIST-800-53R5

- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **IR-5** — Incident Monitoring

CIS-V8

- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

ISO-27001-2022

- **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
T1190	Exploit Public-Facing Application	Initial-Access

Sources

Source	URL	Tier
	https://www.bleepingcomputer.com/news/microsoft/critical-microsoft-...	T3
Disrupting active exploitation of on-premises SharePoint ... - Microsoft	https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting...	T1
Critical Unpatched SharePoint Zero-Day Actively Exploited ...	https://thehackernews.com/2025/07/critical-microsoft-sharepoint-fla...	T3

Source	URL	Tier
Critical Microsoft SharePoint flaw now exploited in attacks	https://x.com/BleepinComputer/status/2034572306295480539	T3
ToolShell: Multi-stage exploit chain of SharePoint vulnerabilities	https://www.cyberbit.com/campaign/toolshell-exploit-chain/	T3

Generated 2026-03-29 18:38 UTC by TJS Security Command Center