Technical Companion

Companion to: On-premises SharePoint RCE actively exploited, and support for 2016/2019 ends in one week
Reference Bulletin Date: July 7, 2026 | For internal use and client technical response

Commands & Syntax Notice: Commands and code in this document are reproduced from cited sources as a reference only. Results may vary based on your environment, OS version, and tooling. Validate in a test environment before running in production.

IOC Notice: Indicators listed here reflect those reported by cited sources at the time of publication and are not exhaustive. Threat actor infrastructure evolves; consult current threat intelligence feeds and your EDR/SIEM for the most complete picture. Absence of these indicators does not confirm a clean environment.

1. Patch Verification

Three steps: confirm your current build, apply the May 2026 update, then confirm the patch landed via Tenable.

Step 1 — Identify Farm Version and Current Build

Action: run in SharePoint Management Shell on each server in the farm:

- Get-SPFarm | Select-Object BuildVersion

Compare against the fixed builds below. Anything lower is vulnerable:

- *SharePoint 2016: 16.0.5552.1002+*
- *SharePoint 2019: 16.0.10417.20128+*
- *Subscription Edition: 16.0.19725.20280+*

Step 2 — Apply the May 2026 Security Update

Action: download and install the KB matching your version from the Microsoft Update Catalog:

- KB5002868 (2016)
- KB5002870 (2019)
- KB5002863 (Subscription Edition)

Post-action: run the SharePoint Products Configuration Wizard on every server application server first, then each web front-end, then iisreset /restart on each front-end. Skipping either step can leave a vulnerable endpoint live even after binaries are updated.

Step 3 — Run Tenable Plugins

Scan with Plugin 314344 to detect CVE-2026-45659 on SharePoint 2016:

- https://www.tenable.com/plugins/nessus/314344

Scan with Plugin 314345 to detect CVE-2026-45659 on SharePoint 2019:

- https://www.tenable.com/plugins/nessus/314345

Scan with Plugin 314338 to detect CVE-2026-45659 on SharePoint Subscription Edition:

- https://www.tenable.com/plugins/nessus/314338

Compromise Detection / Threat Hunt

No CVE-2026-45659-specific IOCs have been published as of this writing (see Section 3). The checks below are behavior-based and drawn from general on-prem SharePoint post-exploitation patterns.

Check 1 — Unexpected Process Trees

w3wp.exe (SharePoint's IIS worker process) spawning PowerShell, cmd.exe, or a scripting host is not normal SharePoint behavior.

- Get-WinEvent -FilterHashtable @{LogName='Security';Id=4688} | Where-Object {$_.Message -match 'w3wp.exe'}

No output = no evidence of this specific pattern; does not rule out compromise — proceed with further checks.

Output present = treat as suspected compromise. Proceed to Section 5.

Check 2 — Unauthorized Web-Accessible Files

Action: inspect _layouts directories on each front-end for .aspx files outside your known baseline deployment.

- Get-ChildItem "C:\inetpub\wwwroot\wss\VirtualDirectories*_layouts\15" -Filter *.aspx | Where-Object {$_.CreationTime -gt (Get-Date).AddDays(-60)}

What constitutes a finding: any .aspx file you can't attribute to a known deployment, customization, or update.

Check 3 — Machine Key and Credential Exposure

This is the most consequential check. Prior on-prem SharePoint campaigns (ToolShell-class) exfiltrated ASP.NET machine keys to persist through patching — a patched-but-previously-exposed server can still be compromised.

If the server was internet-facing at any point before May 12, 2026, rotate machine keys per Microsoft's guidance regardless of confirmed compromise:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45659

If rotation isn't already scheduled, escalate to IR for a compromise assessment before assuming the patch alone resolved exposure.

Check 4 — YARA / Signature Scan

No public YARA rules or file signatures have been released for CVE-2026-45659 as of this writing. Monitor Microsoft MSRC and Tenable Research for updates and apply rules once available.

3. IOC Reference Table

No network-layer IPs, domains, or file hashes tied specifically to CVE-2026-45659 exploitation have been released by CISA, Microsoft, or Tier 1/2 research as of this writing. The entries below reflect general on-prem SharePoint post-exploitation patterns from prior campaigns, not confirmed CVE-2026-45659 indicators.

Type	Indicator	Description	Source
Process	w3wp.exe → cmd.exe / powershell.exe	Anomalous process spawn from SharePoint's IIS worker process; not normal SharePoint behavior.	Community hunting guidance
File Path	_layouts/15/*.aspx (unrecognized)	Unauthorized ASPX web shell dropped via the SharePoint web root following successful deserialization.	Community hunting guidance
Network	Outbound to Cloudflare Tunnel / Zoho Assist / VS Code Server	Remote-access tooling used for persistence in prior on-prem SharePoint campaigns — pattern only, not confirmed for this CVE.	Prior campaign pattern

Note: This table is not a confirmed CVE-2026-45659 IOC set — none have been published as of this bulletin issue date. Update detection logic as CISA, Microsoft, or Tenable releases specifics.

4. Credential and Certificate Rotation Scope

Rotate the following if any affected SharePoint server was internet-facing or broadly accessible before the May 12, 2026, patch was applied.

Credentials to Rotate

- SharePoint farm service account and application pool identity credentials.
- Any account holding Site Member permissions or higher on affected farms — treat as potentially exposed given the low exploitation bar.
- Search service, User Profile service, and other service-application accounts tied to the farm.

Certificates and Keys to Replace

- ASP.NET machine keys on every server in the farm — required to invalidate any persistence mechanism that relied on stolen keys.
- SSL/TLS certificates bound to the SharePoint farm if server compromise is confirmed or suspected.

Account Audit

- Identify dormant or unused accounts with Site Member+ access — these are the most likely entry point if compromised via phishing or credential stuffing.
- Disable accounts with no login activity in the last 90 days that cannot be validated as still required.
- Review authentication logs for SharePoint access from unexpected source IPs or off-hours activity across the exposure window (May 12 – patch date).

5. Incident Response Triggers and Escalation

Confirm Compromise — Immediate Actions

- If process, file, or machine-key indicators return positive: isolate the affected server from the network immediately. Do not remediate in place.
- Preserve a memory capture and disk image before further action. Patching or restarting the server destroys forensic evidence.
- Engage Fortified Health Security IR for forensic triage. SharePoint compromise involving stolen machine keys may require broader identity infrastructure review.

Healthcare-Specific Escalation

- Initiate HIPAA breach determination analysis immediately if PHI-adjacent content was reachable through the compromised site or library.
- The HHS OCR 60-day notification clock starts at confirmed compromise, not at patch completion. Document the compromise confirmation date precisely.
- Preserve all logs and forensic artifacts under legal hold before performing remediation.

Hardening / Reduce Future Attack Surface

- Restrict SharePoint Central Administration and management interfaces to an out-of-band or VPN-only network path.
- Begin migration planning now for any farm on SharePoint 2016 or 2019 — both reach the end of extended support July 14, 2026, seven days from this companion's issue date, with no ESU program announced.
- Apply least-privilege review to Site Member role assignments on a recurring cadence, not just in response to this CVE.

Email: connect@fortifiedhealthsecurity.com | Phone: 615-600-4002