CYXCEL® TRACE

July 2025

TRACE Flash Bulletin

Threat actors are actively exploiting vulnerabilities in on-premise versions of Microsoft SharePoint.

What Has Happened?

Two critical SharePoint vulnerabilities have been under active exploitation since July 18, enabling attackers to upload malicious files and steal cryptographic secrets to aid them in maintaining persistence for future attacks.

CVE-2025-53770 is a critical unauthenticated remote code execution (RCE) vulnerability impacting on-premise versions of Microsoft SharePoint.

CVE-2025-53771 is a path traversal vulnerability leading to server spoofing, which can trick SharePoint into performing unauthorized actions by bypassing path validation and may be used in tandem with CVE-2025-53770 to gain an initial foothold or enhance persistence.

The attacks stem from incomplete fixes from earlier SharePoint vulnerabilities, allowing attackers to exploit even previously patched systems.

Reports from July 23 indicate that over 400 organizations show signs of compromise through exploitation, with a further 8-10,000 servers at risk. Over 200,000 SharePoint services globally could be vulnerable to the exploit.

Attackers are targeting high-value sectors including Government Agencies, Energy and Critical Infrastructure, Educational and Research organizations, Telecoms and Tech, but all businesses running unpatched affected versions should be considered at risk.

The following versions of SharePoint are affected

- SharePoint Server Subscription Licence - All builds prior to (KB5002768)
- SharePoint Server 2019 - Builds earlier than 16.0.10417.20027 (KB5002754)
- SharePoint Server 2016 - Builds earlier than 16.0.5513.1001 (KB5002759)
- Older SharePoint Server versions (2013 and prior) are no longer supported and remain vulnerable

CYXCEL® TRACE

July 2025

Attack Methodology

Initial Access

Threat actors have been exploiting the vulnerability using a specifically crafted HTTP POST request to `/layouts/15/ToolPane.aspx` with a spoofed referrer header `/_layouts/SignOut.aspx` to bypass authentication.

Code Execution

Attackers are then able to execute PowerShell commands and drop a malicious web shell, `spinstall0.aspx`

Key Extraction

The web shell is used to steal cryptographic keys, `ValidationKey` and `DecryptionKey` from Sharepoint's machine configuration

Persistent Access

Attackers can use the stolen keys to forge or decrypt sensitive data and used forged `ViewState` payloads to re-enter the system without detection.

IT security teams should search logs (IIS, Event) for anomalous **`ViewState` payloads or unauthorised **`POST`** requests, Scan file systems for newly added **`aspx`** files. Validate **`machineKey`** integrity and use EDR/XDR tools to search for known IOCs or signatures.*

*Note – this is not intended to be comprehensive remediation guidance, and organisations should follow the latest advice from official sources E.g. Microsoft.

TRACE

CYXCEL® TRACE

July 2025

What Should Organizations Do?

*Priorities for Organizations

- ⓘ Update and patch affected systems immediately – visit the Microsoft website for the latest patches and information (ensure that you are visiting the genuine Microsoft site, other threat actors' prey on significant cyber events, and often spread malware through phishing or malvertising campaigns)
- ⓘ Rotate all cryptographic keys `(ASP.NET, machinekey, certificates, secrets)` after patching
- ⓘ Review audit logs and hosts for malicious payloads or `ViewState` anomalies
- ⓘ Invalidate all sessions and re-issue authentication tokens
- ⓘ Segment and monitor SharePoint servers and look for signs of lateral movement

*Note – this is not intended to be comprehensive remediation guidance, and organisations should follow the latest advice from official sources E.g. Microsoft.

Our Trace team monitors the dark web and digital communications platforms for client exposure and risk across three core areas.

CYXCEL® TRACE

Data, Credentials and Access

We monitor for threats which pose the greatest risks to your organization, searching across stealer marketplaces or initial access brokers offering valid credentials or access to your business, identification of leaked credentials and the offering for sale or exposure of company data.

Organizational Risk

Monitoring for adversarial chat which could indicate an impending or future cyber attack, the registration of domains which may be intended to spoof legitimate company infrastructure.

Supply Chain and Vendor Risks

We dig deeper, monitoring your critical supply chain partners to identify risks which might expose your data or risk downtime which might disrupt your business operations. If a breach does occur within your supply chain, we identify leaked data to allow you to assess the risks posed.

CYXCEL® TRACE

July 2025

Indicators of Compromise

Organizations should monitor for the known indicators of compromise associated with the vulnerability, and monitor for newly published IoCs

SHA-1 File Hashes/Filenames

- f5b60a8ead96703080e73a1f79c3e70ff44df271 – spinstall0.aspx
- fe3a3042890c1f11361368aeb2cc12647a6fdae1 – xxx.aspx
- 76746b48a78a3828b64924f4aedca2e4c49b6735 – App_Web_spinstall0.aspx.9c9699a8.avz5nq6f.dll

IP Addresses (known to be actively exploiting the vulnerabilities)

- 96.9.125[.]147
- 107.191.58[.]76
- 104.238.159[.]149
- 139.59.11[.]66
- 154.223.19[.]106
- 103.151.172[.]92
- 45.191.66[.]77
- 83.136.182[.]237
- 162.248.74[.]92
- 38.54.106[.]11
- 206.166.251[.]228
- 45.77.155[.]170
- 64.176.50[.]109
- 149.28.17[.]188
- 173.239.247[.]32
- 109.105.193[.]76
- 2.56.190[.]139
- 141.164.60[.]10
- 124.56.42[.]75

*Note – this is not intended to be comprehensive remediation guidance, and organisations should follow the latest advice from official sources E.g. Microsoft.

Our Trace team monitors the dark web and digital communications platforms for client exposure and risk across three core areas.

CYXCEL® TRACE

Data, Credentials and Access

We monitor for threats which pose the greatest risks to your organization, searching across stealer marketplaces or initial access brokers offering valid credentials or access to your business, identification of leaked credentials and the offering for sale or exposure of company data.

Organizational Risk

Monitoring for adversarial chat which could indicate an impending or future cyber attack, the registration of domains which may be intended to spoof legitimate company infrastructure.

Supply Chain and Vendor Risks

We dig deeper, monitoring your critical supply chain partners to identify risks which might expose your data or risk downtime which might disrupt your business operations. If a breach does occur within your supply chain, we identify leaked data to allow you to assess the risks posed.