ToolShell – Microsoft SharePoint Zero-Day Under Active Attack

TL;DR

A zero-day vulnerability in on-premises Microsoft SharePoint Server (CVE-2025-53770) is being actively exploited in the wild.

The flaw allows unauthenticated remote code execution and theft of cryptographic keys, allowing for full compromise of SharePoint environments.

Microsoft has released partial patches, but many systems remain exposed.

Overview

A new zero-day vulnerability (CVE-2025-53770, CVSS 9.8) affecting Microsoft SharePoint Server is being exploited by unknown threat actors. The flaw allows remote attackers to execute code and steal digital machine keys without needing login credentials. Microsoft SharePoint Online is unaffected, but self-hosted SharePoint servers are at risk.

CVE-2025-53770 is a deserialization flaw in on-premises SharePoint Server that allows remote code execution with no authentication. Attackers can leverage this vulnerability to extract cryptographic machine keys, impersonate legitimate server requests, install webshells, and maintain long-term access. The exploit is being chained with CVE-2025-53771 in some cases, which acts as an authentication bypass.

Affected Products

- Microsoft SharePoint Server 2016 (Patch Pending)
- Microsoft SharePoint Server 2019 (Patch Available)
- Microsoft SharePoint Server Subscription Edition (Patch Available)
- Not affected – SharePoint Online (Microsoft 365)

Exploitation began prior to patch availability, and internet scans show that thousands of organizations may still be vulnerable. CVE-2025-53770 affects versions as old as SharePoint Server 2016.

The exploit has been named “ToolShell” and is considered severe due to its ability to grant full server access. While some patches are now available, not all versions (e.g., SharePoint 2016) have fixes yet. Over 100 organizations in the U.S. and Germany have been targeted, with confirmed victims including U.S. federal agencies, universities, and energy companies. Although patching alone may not fully protect against this vulnerability, Aspire still strongly recommends applying the update immediately.

Aspire Protects

- **Patch** – Organizations should patch this vulnerability immediately. See Microsoft's advisory and Microsoft's customer guidance blog for more information:
  - If AMSI is enabled - Apply the July 2025 security update immediately and rotate SharePoint ASP.NET machine keys post-patching.
  - If AMSI is not enabled - Disconnect vulnerable SharePoint servers from the internet until patches can be applied.
  - Enable Microsoft Defender Antivirus and configure AMSI Full Mode integration for SharePoint.
  - Deploy Microsoft Defender for Endpoint to detect post-exploit activity.
  - Check for malicious files like spinstall0.aspx, unusual PowerShell commands from w3wp.exe, and suspicious activity in the SharePoint LAYOUTS directory.
- Patching is always a best practice, but in this case, organizations should take an assumed breach approach. Instead of waiting for signs of an attack, operate under the mindset that the attacker is already inside your network:
  - Hunt for signs of compromise (IoCs, strange behavior, etc.).
  - Rotate credentials or keys that could have been stolen.
  - Increase monitoring and logging.
  - Isolate systems that are at high risk.
  - Verify integrity of apps and files (not just patch and move on).

TTPs to Watch

Initial Access
- Exploit Public-Facing Application [T1190] – The attacker may have used the deserialization flaw in SharePoint's LAYOUTS endpoint to gain unauthenticated access.

Persistence
- Server Software Component [T1505.003] – Web shells and malicious ASPX pages dropped into the SharePoint web directory.

Defense Evasion
- Masquerading [T1036] – Use of encoded PowerShell commands and file names mimicking legitimate SharePoint components.

Credential Access
- Steal Application Access Token [T1528] – Theft of SharePoint machine keys used to forge server-side requests.

IoCs

Webshell path

- /_layouts/15/ToolPane.aspx?DisplayMode=Edit

IPv4

- 107[.]191[.]58[.]76
- 104[.]238[.]159[.]149
- 96[.]9[.]125[.]147

File

- spinstall0.aspx

Behavior

- PowerShell spawned by w3wp.exe with encoded commands

Targeted Industries

The attacks are hitting industries that rely on SharePoint for internal operations, with government, education, and energy sectors already confirmed among the victims.

- Healthcare
- Financial
- Government
- Manufacturing
- Education
- Technology
- Energy

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security

professionals to identify and respond to threats across a broader attack surface.
    - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
    - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
    - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
    - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

CVE-2025-53770 - Security Update Guide - Microsoft - Microsoft SharePoint Server Remote Code Execution Vulnerability

Customer guidance for SharePoint vulnerability CVE-2025-53770 | MSRC Blog | Microsoft Security Response Center

NVD - CVE-2025-53770

NVD - CVE-2025-53771

Zero-day exploitation in the wild of Microsoft SharePoint servers via CVE-2025-53770

Toolshell: Large-scale exploitation of new SharePoint RCE vulnerability chain identified - LevelBlue - Open Threat Exchange