SharePoint "ToolShell" Vulnerability: CVE-2025-53770

July 21st, 2025

Executive Summary

CVE-2025-53770 is a critical Remote Code Execution (RCE) vulnerability in multiple versions of on-premises Microsoft SharePoint Server with a CVSS v3.1 base score of 9.8. Deserialization of untrusted data in on-premises Microsoft SharePoint Server allows an unauthorized attacker to execute code over a network. Microsoft is aware that an exploit for CVE-2025-53770 exists in the wild.[1] SRA has observed and responded to exploitation attempts in multiple client environments.

This vulnerability affects on-premises SharePoint Servers only. SharePoint Online in Microsoft 365 is not impacted. This exploitation activity, publicly reported as "ToolShell," provides unauthenticated access to systems and enables malicious actors to fully access SharePoint content, including file systems and internal configurations, and execute code over the network.[2] CVE-2025-53770 was disclosed following active exploitation identified by Eye Security on July 18, 2025.[3]

Microsoft has released security updates for customers using SharePoint Subscription Edition and SharePoint 2019. At the time of writing, no update is yet available for SharePoint 2016. Microsoft notes, *"We are working on security updates for supported versions of SharePoint 2019 and SharePoint 2016. Please check this blog for updates"*. CVE-2025-53770 was added to CISA's Known Exploited Vulnerabilities (KEV) catalog on July 20, 2025.

Impact

The ToolShell exploit chain allows attackers to achieve remote code execution on SharePoint servers without authentication. Attackers extract ASP.NET MachineKeys from the server, specifically the ValidationKey and DecryptionKey, and use them to craft forged __VIEWSTATE payloads. These payloads are accepted as legitimate by SharePoint, allowing attackers to maintain access and run arbitrary commands without detection.[3]

Successful exploitation grants attackers access to SharePoint content, system files, and configurations, and potentially may allow attackers to move laterally across the Windows Domain. The stolen cryptographic keys enable persistent access even after patching. According to Eye Security, "Patching alone does not solve the issue; you need to rotate the cryptographic material allowing all future IIS tokens that can be created by the malicious actor to become invalid."[3] Because SharePoint often connects to core services like Outlook, Teams, and OneDrive, a breach of SharePoint can quickly lead to data theft, password harvesting, and lateral movement across the environment.

Affected Products

- Microsoft SharePoint Server Subscription Edition
- Microsoft SharePoint Server 2019

Copyright © 2025. Security Risk Advisors Intl, LLC. All Rights Reserved

- Microsoft SharePoint Enterprise Server 2016
- SharePoint Online (Microsoft 365) is NOT affected

Safeguards/Recommendations

Organizations should take steps to protect themselves from further risk as follows:

- Review official Microsoft guidance related to CVE-2025-53770.
- Configure Antimalware Scan Interface (AMSI) in SharePoint, enable Full Mode for optimal protection, and deploy Microsoft Defender AV on all SharePoint servers.
    - If AMSI cannot be enabled, disconnect affected products from the service that are public facing on the internet until official mitigations are available.
- Use or upgrade to supported versions of on-premises Microsoft SharePoint Server.
    - Supported versions: SharePoint Server 2016, 2019, & SharePoint Subscription Edition
- Install July 2025 Security Updates.
- Rotate SharePoint Server ASP.NET machine keys
    - See Microsoft guidance for assistance
- Monitor for malicious activity, especially POST requests to `/_layouts/15/ToolPane.aspx`

Microsoft provides hunting queries organizations can use in Microsoft Defender to aid in detection of exploit attempts. SRA has completed preliminary searches for these queries within XDR/ESOC client environments and has notified any affected customers.

Additional queries can be found in the following source.

IOCs

Source: Eye Security - SharePoint Under Siege: ToolShell Mass Exploitation

- 107.191.58[.]76 – first exploit wave US-based source IP responsible for active exploitation on 18th of July around 18:06 UTC deploying spinstall0.aspx
- 104.238.159[.]149 – second exploit wave US-based source IP responsible for active exploitation on 19th of July around 07:28 UTC
- 96.9.125[.]147 – shared by PaloAlto Unit42
- 103.186.30[.]186 – shared on X by @andrewdanis
- Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101 Firefox/120.0 – user agent string used in active exploitation on 18th & 19th of July 2025
- Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:120.0)+Gecko/20100101+Firefox/120.0 – URL-encoded user agent string for IIS log searches
- /_layouts/15/ToolPane.aspx?DisplayMode=Edit&a=/ToolPane.aspx – POST path used to trigger exploit and push Sharpyshell related to CVE-2025-49706 and/or CVE-2025-53770
- Referer: /_layouts/SignOut[.]aspx – exact HTTP header used in exploiting ToolPane.aspx inside POST request related to CVE-2025-53770
- GET request to malicious ASPX file in /_layouts/15/spinstall0.aspx – aspx crypto dumper used by CVE-2021-28474 with tool ysoserial to get RCE on SharePoint
- 92bb4ddb98eeaf11fc15bb32e71d0a63256a0ed826a03ba293ce3a8bf057a514 – SHA256 hash of spinstall0[.]aspx crypto dumper probably created with Sharpyshell

Copyright © 2025. Security Risk Advisors Intl, LLC. All Rights Reserved

- C:\PROGRA~1\COMMON~1\MICROS~1\WEBSER~1\16\TEMPLATE\LAYOUTS\spinstall0.aspx – location of the malicious aspx file on Windows Servers running SharePoint

Source: SOCRadar - ToolShell Campaign: New SharePoint Zero-Day

- aspx files like spinstall0[.]aspx in LAYOUTS directories
- POST requests to /ToolPane[.]aspx with unusual parameters
- Abnormal __VIEWSTATE payloads or signature anomalies
- IP activity from 107.191.58[.]76, 104.238.159[.]149, 96.9.125[.]147
- URL-encoded Firefox user-agent strings in logs
- Noted file hashes:
    - 4a02a72aedc3356d8cb38f01f0e0b9f26ddc5ccb7c0f04a561337cf24aa84030
    - b39c14becb62aeb55df7fd55c814afbb0d659687d947d917512fe67973100b70
    - fa3a74a6c015c801f5341c02be2cbdfb301c6ed60633d49fc0bc723617741af7

References

- Microsoft Security Response Center - Customer guidance for SharePoint vulnerability CVE-2025-53770
- CISA Alert - Microsoft Releases Guidance on Exploitation of SharePoint Vulnerability (CVE-2025-53770)
- Eye Security - SharePoint Under Siege: ToolShell Mass Exploitation
- BleepingComputer - Microsoft SharePoint zero-day exploited in RCE attacks
- Canadian Centre for Cyber Security - Vulnerability impacting Microsoft SharePoint Server (CVE-2025-53770)
- SOCRadar - ToolShell Campaign: New SharePoint Zero-Day
- NVD - CVE-2025-53770
- GitHub - MICROSOFT SHAREPOINT VULNERABILITIES - CVE-2025-49704, CVE-2025-49706, CVE-2025-53770 AND CVE-2025-53771

Copyright © 2025. Security Risk Advisors Intl, LLC. All Rights Reserved