

HiveForce Labs

# THREAT ADVISORY

 **VULNERABILITY REPORT**

## Zero Day Watch CVE-2025-53770 Turns SharePoint into a Pivot Point

Date of Publication

July 21, 2025

Admiralty Code

A1

TA Number

TA2025227

# Summary

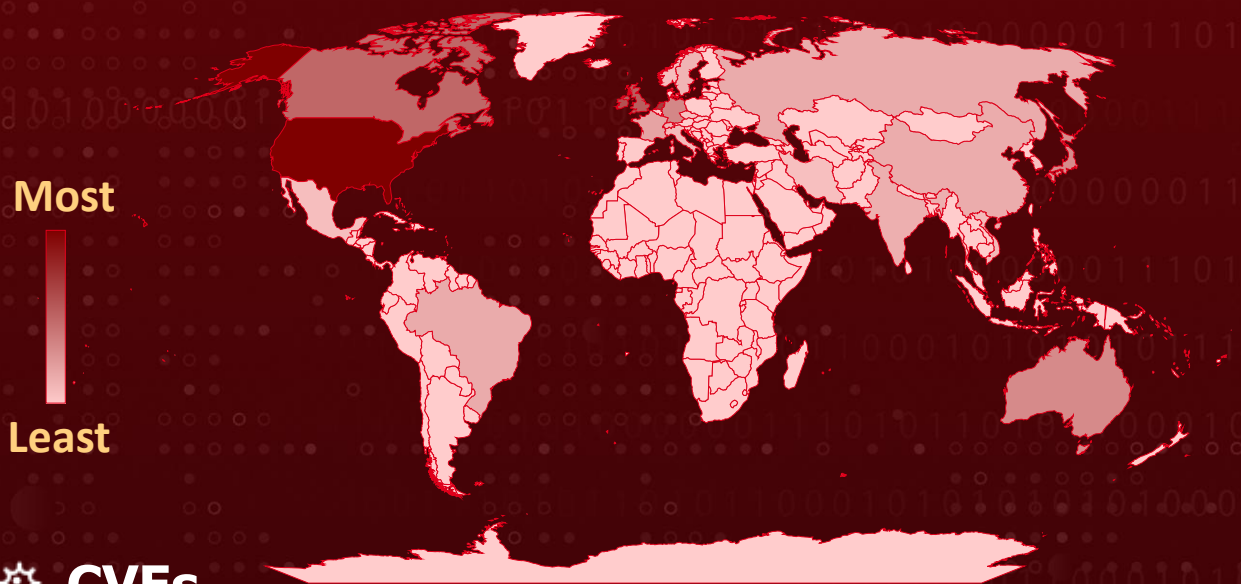
**Attack Commenced:** 18 July 2025

**Affected Product:** Microsoft SharePoint Server

**Top Targeted Countries:** United States, Netherlands, Ireland, United Kingdom, Canada




**Impact:** A high-impact zero-day vulnerability, tracked as CVE-2025-53770, is actively being exploited in the wild, targeting on-premises Microsoft SharePoint Servers. This newly uncovered flaw enables attackers to sidestep existing security patches and gain unauthorized access to critical systems. Organizations with internet-facing SharePoint environments are strongly urged to assume compromise and move swiftly with proactive containment and comprehensive remediation.

## 🔪 Targeted Regions



## ⚙ CVEs

| CVE            | NAME  | AFFECTED PRODUCT     | ZERO-DAY | CISA KEV | PATCH |
|----------------|---|----------------------|----------|----------|-------|
| CVE-2025-53770 | Microsoft SharePoint Server Remote Code Execution Vulnerability | Microsoft SharePoint | ✅        | ✅        | ✅     |
| CVE-2025-53771 | Microsoft SharePoint Server Spoofing Vulnerability              | Microsoft SharePoint | ❌        | ❌        | ✅     |
| CVE-2025-49706 | Microsoft SharePoint Server Spoofing Vulnerability              | Microsoft SharePoint | ❌        | ❌        | ✅     |

| CVE                            | NAME   | AFFECTED PRODUCT     | ZERO-DAY  | CISA KEV  | PATCH   |
|--------------------------------|--|----------------------|---|---|---|
| <a href="#">CVE-2025-49704</a> | Microsoft SharePoint Remote Code Execution Vulnerability | Microsoft SharePoint |  |  |  |

# Vulnerability Details

## #1

A newly identified zero-day vulnerability, designated CVE-2025-53770, has surfaced as part of a widespread and active exploitation campaign targeting on-premises deployments of Microsoft SharePoint Server. This flaw is considered a variant of CVE-2025-49706, a spoofing vulnerability previously addressed in Microsoft's July 2025 Patch Tuesday release.

## #2

CVE-2025-53770 centers around the unsafe deserialization of untrusted data, enabling unauthenticated remote code execution (RCE). The attack vector likely involves unauthenticated HTTP POST requests to key SharePoint endpoints, particularly those located under the `/_layouts/15/` directory, which contains critical application pages.

## #3

In observed cases, a crafted POST request was sent to `/_layouts/15/ToolPane.aspx`, accompanied by an HTTP Referer header set to `/_layouts/SignOut.aspx`. This manipulation triggers an authentication bypass, which is then leveraged to execute malicious code. Successful exploitation can reveal the server's MachineKey configuration, allowing attackers to forge requests that bypass authentication controls entirely.

## #4

Compounding the threat, a closely related vulnerability, tracked CVE-2025-53771, was disclosed. This flaw arises from improper restriction of directory traversal in SharePoint, allowing authorized attackers to conduct spoofing attacks across the network. Both vulnerabilities are related to earlier flaws, [CVE-2025-49704](#) and CVE-2025-49706, which could be chained to achieve remote code execution.

## #5

This exploit chain, collectively known as ToolShell, was demonstrated in a successful attack during Pwn2Own Berlin in May 2025. Although Microsoft addressed the ToolShell vulnerabilities in its July patch cycle, threat actors have quickly adapted, developing new methods to circumvent those fixes.

# #6

Organizations with internet-exposed, on-premises SharePoint servers should assume potential compromise. Effective remediation requires a comprehensive incident response, including log review, threat hunting, and possible architectural adjustments. SharePoint integrates deeply with Microsoft services like Office, Teams, OneDrive, and Outlook. A successful breach can provide lateral access across the network, escalating an initial intrusion into a broader compromise of sensitive systems and data.

## Vulnerability

| CVE ID         | AFFECTED PRODUCTS   | AFFECTED CPE  | CWE ID                      |
|----------------|---|---|-----------------------------|
| CVE-2025-53770 | Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016, and Microsoft SharePoint Server Subscription Edition | cpe:2.3:a:microsoft:sharepoint:*:*:*:*:*:*<br>cpe:2.3:a:microsoft:sharepoint_enterprise_server:-:*:*:*:*:*: | CWE-502                     |
| CVE-2025-53771 | Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016, and Microsoft SharePoint Server Subscription Edition | cpe:2.3:a:microsoft:sharepoint:*:*:*:*:*:*<br>cpe:2.3:a:microsoft:sharepoint_enterprise_server:-:*:*:*:*:*: | CWE-707<br>CWE-22<br>CWE-20 |
| CVE-2025-49706 | Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016, Microsoft SharePoint Server Subscription Edition     | cpe:2.3:a:microsoft:sharepoint:*:*:*:*:*:*<br>cpe:2.3:a:microsoft:sharepoint_enterprise_server:-:*:*:*:*:*: | CWE-287                     |
| CVE-2025-49704 | Microsoft SharePoint Enterprise Server: 2016 - 2019   | cpe:2.3:a:microsoft:sharepoint:*:*:*:*:*:*<br>cpe:2.3:a:microsoft:sharepoint_enterprise_server:-:*:*:*:*:*: | CWE-94                      |

## Recommendations



**Enable and Configure AMSI Protection:** Strongly recommended to enable the Antimalware Scan Interface (AMSI) and configure it in Full Mode on all SharePoint servers. This enables real-time protection from malicious deserialization and post-exploit activity by integrating with Microsoft Defender Antivirus. AMSI is enabled by default in the September 2023 update for SharePoint 2016/2019 and in Version 23H2 for SharePoint Subscription Edition. If AMSI cannot be enabled, the server should be disconnected from the internet until updates are applied.





**Rotate Machine Keys After Mitigation:** After applying the latest security patches or enabling AMSI, it is critical to rotate the ASP.NET machine keys across all SharePoint servers. This step ensures that any compromised keys can no longer be reused by attackers. Key rotation can be done using the Update-SPMachineKey PowerShell cmdlet or by running the Machine Key Rotation Job in Central Administration. An IIS restart (iisreset) is required after rotation to apply the new keys effectively.



**Monitor for Exploitation with Advanced Hunting:** Look for indicators such as the creation of spinstall0.aspx in SharePoint LAYOUTS directories or PowerShell scripts launched by w3wp.exe containing encoded commands.



**Vulnerability Management:** This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.



## Potential MITRE ATT&CK TTPs

|  |  |   |  |
|--|--|---|--|
| <b><u>TA0001</u></b><br>Initial Access                   | <b><u>TA0002</u></b><br>Execution                        | <b><u>TA0003</u></b><br>Persistence                 | <b><u>TA0006</u></b><br>Credential Access        |
| <b><u>TA0007</u></b><br>Discovery                        | <b><u>TA0008</u></b><br>Lateral Movement                 | <b><u>TA0011</u></b><br>Command and Control         | <b><u>TA0010</u></b><br>Exfiltration             |
| <b><u>T1190</u></b><br>Exploit Public-Facing Application | <b><u>T1059</u></b><br>Command and Scripting Interpreter | <b><u>T1059.001</u></b><br>PowerShell               | <b><u>T1505</u></b><br>Server Software Component |
| <b><u>T1505.003</u></b><br>Web Shell                     | <b><u>T1552.001</u></b><br>Credentials In Files          | <b><u>T1083</u></b><br>File and Directory Discovery | <b><u>T1018</u></b><br>Remote System Discovery   |
| <b><u>T1021.002</u></b><br>SMB/Windows Admin Shares      | <b><u>T1071.001</u></b><br>Web Protocols                 |   |  |

## ⚔ Indicators of Compromise (IOCs)

| TYPE        | VALUE  |
|-------------|--|
| <b>IPv4</b> | 107[.]191[.]58[.]76,<br>104[.]238[.]159[.]149,<br>96[.]9[.]125[.]147,<br>172[.]174[.]82[.]132,<br>103[.]186[.]30[.]186 |



| TYPE                       | VALUE   |
|----------------------------|---|
| <b>HTTP POST URI</b>       | /_layouts/15/ToolPane.aspx?DisplayMode=Edit&a=/ToolPane.aspx  |
| <b>HTTP Referer Header</b> | /_layouts/SignOut.aspx  |
| <b>SHA256</b>              | 92bb4ddb98eeaf11fc15bb32e71d0a63256a0ed826a03ba293ce3a8bf057a514,<br>4a02a72aedc3356d8cb38f01f0e0b9f26ddc5ccb7c0f04a561337cf24aa84030,<br>b39c14becb62aeb55df7fd55c814afbb0d659687d947d917512fe67973100b70,<br>fa3a74a6c015c801f5341c02be2cbdfb301c6ed60633d49fc0bc723617741af7 |
| <b>Filesystem Path</b>     | C:\PROGRA~1\COMMON~1\MICROS~1\WEBSE~1\16\TEMPLATE\LA<br>YOUTS\spinstall0.aspx,<br>C:\PROGRA~1\COMMON~1\MICROS~1\WEBSE~1\15\TEMPLATE\LA<br>YOUTS\spinstall0.aspx   |

## Patch Details

Microsoft has released security updates that fully mitigate CVE-2025-53770 and CVE-2025-53771 for the following SharePoint versions. Customers are strongly advised to apply these updates without delay:

SharePoint Server Subscription Edition - Security Update: [KB5002768](#)

SharePoint Server 2019 - Security Update: [KB5002754](#)

For SharePoint Server 2016, a security update addressing these vulnerabilities is not yet available. Customers using this version should closely monitor Microsoft's official guidance for release updates and consider applying interim mitigation measures as recommended.

Links:

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53770>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53771>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-49706>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-49704>

## References

<https://msrc.microsoft.com/blog/2025/07/customer-guidance-for-sharepoint-vulnerability-cve-2025-53770/>

<https://www.cisa.gov/news-events/alerts/2025/07/20/microsoft-releases-guidance-exploitation-sharepoint-vulnerability-cve-2025-53770>

<https://research.eye.security/sharepoint-under-siege/>

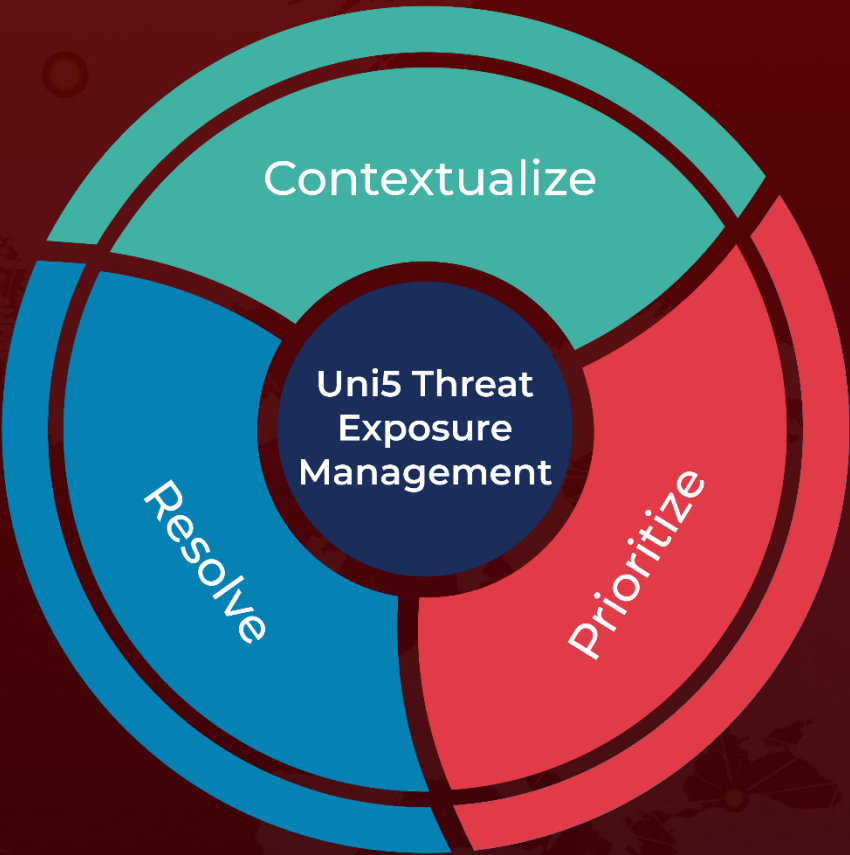
<https://github.com/PaloAltoNetworks/Unit42-timely-threat-intel/blob/main/2025-07-19-Microsoft-SharePoint-vulnerabilities-CVE-2025-49704-and-49706.txt>

<https://hivepro.com/threat-advisory/microsofts-july-2025-patch-tuesday-addresses-130-vulnerabilities/>

# What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON  
**July 21, 2025 • 11:00 AM**

© 2025 All Rights are Reserved by Hive Pro



More at [www.hivepro.com](http://www.hivepro.com)