Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

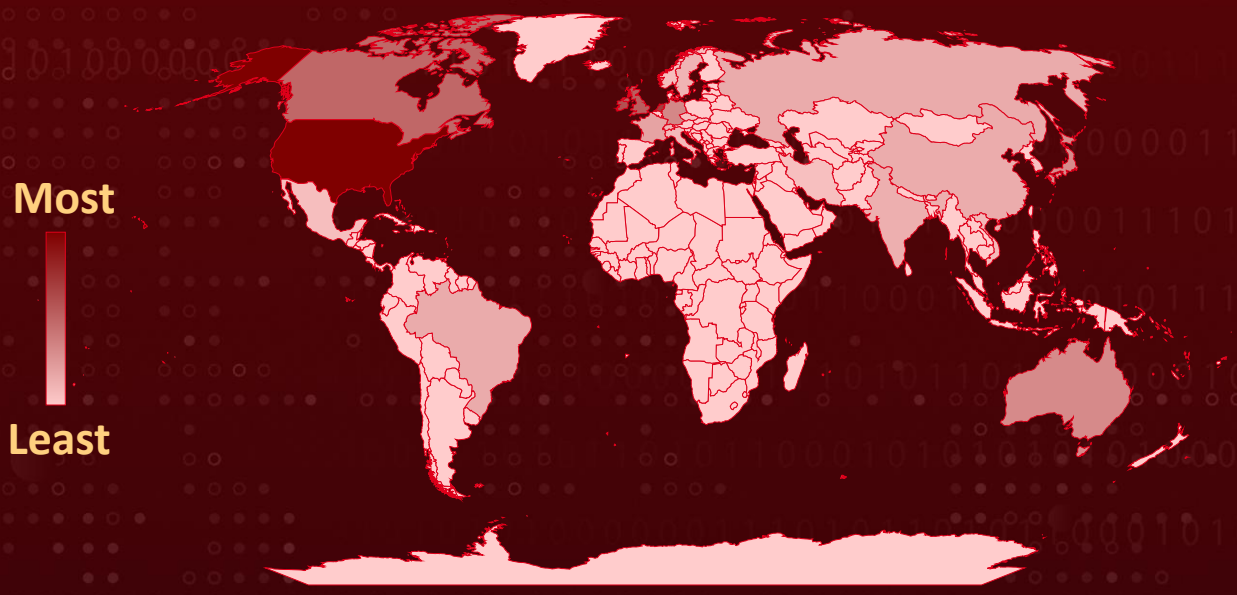
Zero Day Watch CVE-2025-53770 Turns SharePoint into a Pivot Point

Date of Publication	Last Update Date	Admiralty Code	TA Number
July 21, 2025	August 4, 2025	A1	TA2025227

Summary

Attack Commenced: July 7, 2025
Affected Product: Microsoft SharePoint Server
Threat Actors: Linen Typhoon, Violet Typhoon, Storm-2603
Ransomware: Warlock, 4L4MD4R
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. With three China-backed threat actors exploiting these weaknesses, organizations operating internet-facing SharePoint environments are strongly advised to assume compromise and take immediate action through proactive containment and thorough remediation efforts.

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	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-49706	Microsoft SharePoint Server Spoofing Vulnerability	Microsoft SharePoint	✗	✓	✓
CVE-2025-49704	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 Two China-based nation-state groups, Linen Typhoon (aka APT27, EMISSARY PANDA) and Violet Typhoon (aka APT31, JUDGMENT PANDA), have been observed exploiting these vulnerabilities to target internet-exposed SharePoint servers for espionage and intelligence gathering. Additionally, Storm-2603, a likely China-linked threat actor previously associated with Warlock and LockBit ransomware, has been exploiting the same vulnerabilities to conduct financially motivated ransomware attacks.

#7 Storm-2603 leveraged access obtained through CVE-2025-53770 to deploy Warlock ransomware. During post-exploitation, the threat actor was observed modifying Group Policy Objects (GPOs) to automate the distribution of ransomware payloads across compromised networks, significantly accelerating lateral movement and system-wide encryption.

#8 On July 27, 2025, an unsuccessful exploitation attempt using an encoded PowerShell command uncovered the deployment of 4L4MD4R ransomware, a variant of the open-source Mauri870 ransomware. The PowerShell payload aimed to disable real-time monitoring and circumvent certificate validation. This operation led to the detection of a loader that downloaded and executed the ransomware from a command-and-control server.

#9 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:*:*:*:*:*:*:*:* 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:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:sharepoint_enterprise_server:-:*:*:*:*:*:*:*	CWE-707 CWE-22 CWE-20

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-49706	Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016, Microsoft SharePoint Server Subscription Edition	cpe:2.3:a:microsoft:sharepoint:*:*:*:*:*:*:*:* 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:*:*:*:*:*:*:*:* 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

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0006** Credential Access	**TA0007** Discovery	**TA0008** Lateral Movement
TA0009 Collection	**TA0011** Command and Control	**TA0010** Exfiltration	**TA0040** Impact
T1190 Exploit Public-Facing Application	**T1059** Command and Scripting Interpreter	**T1059.001** PowerShell	**T1059.003** Windows Command Shell
T1505.003 Web Shell	**T1552.001** Credentials In Files	**T1083** File and Directory Discovery	**T1018** Remote System Discovery
T1021.002 SMB/Windows Admin Shares	**T1071.001** Web Protocols	**T1033** System Owner/User Discovery	**T1505** Server Software Component
T1569 System Services	**T1569.002** Service Execution	**T1543** Create or Modify System Process	**T1543.003** Windows Service
T1047 Windows Management Instrumentation	**T1505.004** IIS Components	**T1053.005** Scheduled Task	**T1484.001** Group Policy Modification
T1620 Reflective Code Loading	**T1562.001** Disable or Modify Tools	**T1112** Modify Registry	**T1003.001** LSASS Memory
T1570 Lateral Tool Transfer	**T1119** Automated Collection	**T1005** Data from Local System	**T1090** Proxy
T1486 Data Encrypted for Impact			

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	107[.]191[.]58[.]76, 96[.]9[.]125[.]147, 172[.]174[.]82[.]132, 103[.]186[.]30[.]186, 131[.]226[.]2[.]6, 134[.]199[.]202[.]205, 104[.]238[.]159[.]149, 188[.]130[.]206[.]168, 65[.]38[.]121[.]198, 145[.]239[.]97[.]206, 139[.]144[.]199[.]41, 89[.]46[.]223[.]88, 45[.]77[.]155[.]170, 154[.]223[.]19[.]106, 185[.]197[.]248[.]131, 149[.]40[.]50[.]15, 64[.]176[.]50[.]109, 149[.]28[.]124[.]70, 206[.]166[.]251[.]228, 95[.]179[.]158[.]42, 86[.]48[.]9[.]38, 128[.]199[.]240[.]182, 212[.]125[.]27[.]102, 91[.]132[.]95[.]60
HTTP POST URI	/_layouts/15/ToolPane.aspx?DisplayMode=Edit&a=/ToolPane.aspx
HTTP Referer Header	/_layouts/SignOut.aspx
URLs	c34718cbb4c6[.]ngrok-free[.]app/file[.]ps1, msupdate[.]updatemicfosoft[.]com, hxxps[:]//ice[.]theinnovationfactory[.]it/static/4l4md4r[.]exe
Email	m4_cruise[@]proton[.]me
Bitcoin wallet Address	bc1qqxqe9vsvjmjqc566fgqsgnhlh87fckwegmtg6p
Domain	bpp[.]theinnovationfactory[.]it
SHA256	92bb4ddb98eeaf11fc15bb32e71d0a63256a0ed826a03ba293ce3a8bf057a514,

TYPE	VALUE
SHA256	4a02a72aedc3356d8cb38f01f0e0b9f26ddc5ccb7c0f04a561337cf24aa84030, b39c14becb62aeb55df7fd55c814afbb0d659687d947d917512fe67973100b70, fa3a74a6c015c801f5341c02be2cbdfb301c6ed60633d49fc0bc723617741af7, 24480dbe306597da1ba393b6e30d542673066f98826cc07ac4b9033137f37dbf, b5a78616f709859a0d9f830d28ff2f9dbbb2387df1753739407917e96dadf6b0, c27b725ff66fdfb11dd6487a3815d1d1eba89d61b0e919e4d06ed3ac6a74fe94, 1eb914c09c873f0a7bcf81475ab0f6bdfaccc6b63bf7e5f2dbf19295106af192, 4c1750a14915bf2c0b093c2cb59063912dfa039a2adfe6d26d6914804e2ae928, 83705c75731e1d590b08f9357bc3b0f04741e92a033618736387512b40dab060, f54ae00a9bae73da001c4d3d690d26ddf5e8e006b5562f936df472ec5e299441, b180ab0a5845ed619939154f67526d2b04d28713fcc1904fbd666275538f431d, 6753b840cec65dfba0d7d326ec768bff2495784c60db6a139f51c5e83349ac4d, 7ae971e40528d364fa52f3bb5e0660ac25ef63e082e3bbd54f153e27b31eae68, 567cb8e8c8bd0d909870c656b292b57bcb24eb55a8582b884e0a228e298e7443, 445a37279d3a229ed18513e85f0c8d861c6f560e0f914a5869df14a74b679b86, ffbc9dfc284b147e07a430fe9471e66c716a84a1f18976474a54bee82605fa9a, 6b273c2179518dacb1218201fd37ee2492a5e1713be907e69bf7ea56ceca53a5, c2c1fec7856e8d49f5d49267e69993837575dbbec99cd702c5be134a85b2c139, 6f6db63ece791c6dc1054f1e1231b5bbcf6c051a49bad0784569271753e24619, d6da885c90a5d1fb88d0a3f0b5d9817a82d5772d5510a0773c80ca581ce2486d, 62881359e75c9e8899c4bc9f452ef9743e68ce467f8b3e4398bebacde9550dea, da8de7257c6897d2220cdf9d4755b15aeb38715807e3665716d2ee761c266fdb, 33067028e35982c7b9fdcfe25eb4029463542451fdff454007832cf953feaf1e,

TYPE	VALUE
SHA256	390665bdd93a656f48c463bb6c11a4d45b7d5444bdd1d1f7a5879b0f6f9aac7e, 66af332ce5f93ce21d2fe408dffd49d4ae31e364d6802fff97d95ed593ff3082, 7baf220eb89f2a216fcb2d0e9aa021b2a10324f0641caf8b7a9088e4e45bec95
File Path	C:\PROGRA~1\COMMON~1\MICROS~1\WEBSER~1\16\TEMPLATE\LAYOUTS\spinstall0.aspx, C:\PROGRA~1\COMMON~1\MICROS~1\WEBSER~1\15\TEMPLATE\LAYOUTS\spinstall0.aspx, C:\Program Files\Common Files\microsoft shared\Web Server Extensions\16\TEMPLATE\LAYOUTS\debug_dev.js \1[5-6]\TEMPLATE\LAYOUTS\debug_dev.js
Filename	Spinstall0.aspx, IIS_Server_dll.dll, SharpHostInfo.x64.exe, xd.exe, debug_dev.js
TOR Address	elqfbcx5nofwtqfookqml7ltx2g6q6tmddys6e25vgu3al2meim6cbqd[.]onion, zfytizegsze6uiswodhbaalyy5rawaytv2nzyzdkt3susbewviqqh7yd[.]onion

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://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/

https://unit42.paloaltonetworks.com/microsoft-sharepoint-cve-2025-49704-cve-2025-49706-cve-2025-53770/

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

https://github.com/mauri870/ransomware/tree/master

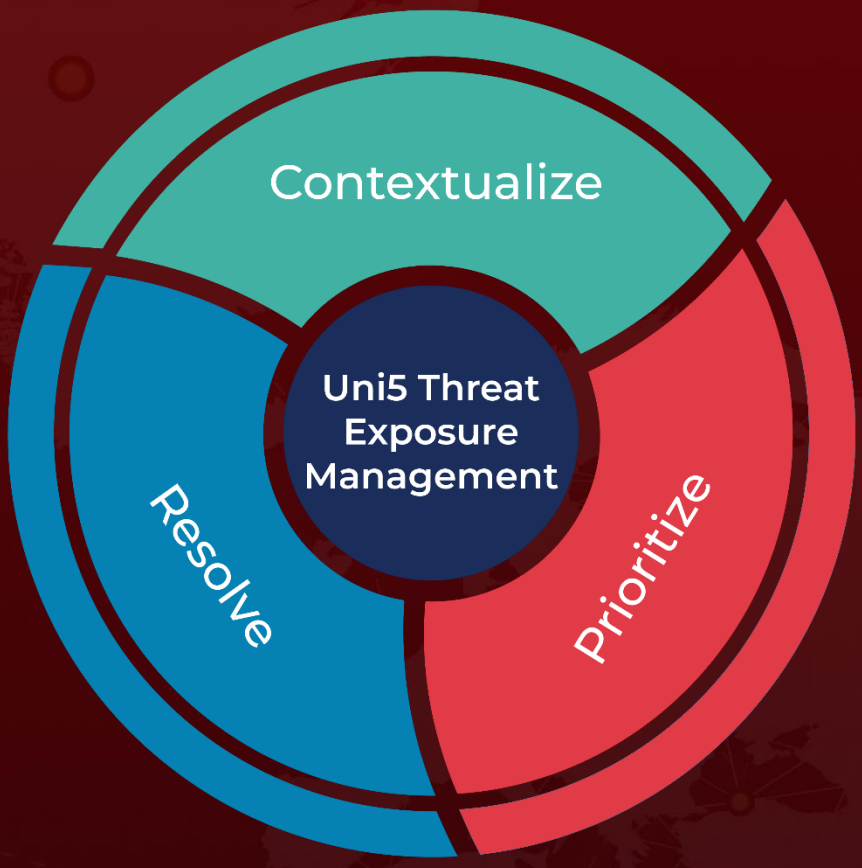
https://hivepro.com/threat-advisory/microsofts-july-2025-patch-tuesday-addresses-130-vulnerabilities/

https://hivepro.com/threat-advisory/lockbit-ransomware-evolving-tactics-and-pervasive-impact-in-2023/

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

More at www.hivepro.com