NVIDIA INCEPTION PROGRAM

SAPTANG™
Proactive Threat Defence

Risk Advisory: Your Organization May Be at Risk — Active Exploitation of Microsoft SharePoint Vulnerabilities (ToolShell)

Date: 24/07/2025

C3iHub | National Centre of Excellence in Cybersecurity Technology and Entrepreneurship | Microsoft for Startups Founders Hub

1. Executive Summary

A set of critical, actively exploited vulnerabilities in Microsoft SharePoint Server (CVE-2025-53770 and CVE-2025-53771) have been weaponized by advanced threat actors and are now being used in real-world attacks. These vulnerabilities enable unauthenticated remote code execution (RCE) and persistence mechanisms that allow attackers to compromise systems deeply and silently.

Your organization is potentially exposed to this threat, if:

- You are operating on-premises SharePoint Servers (2016/2019/Subscription Edition).
- These servers are internet-facing or not fully patched.
- Security tools are not monitoring SharePoint-specific activity paths, which attackers are now exploiting.

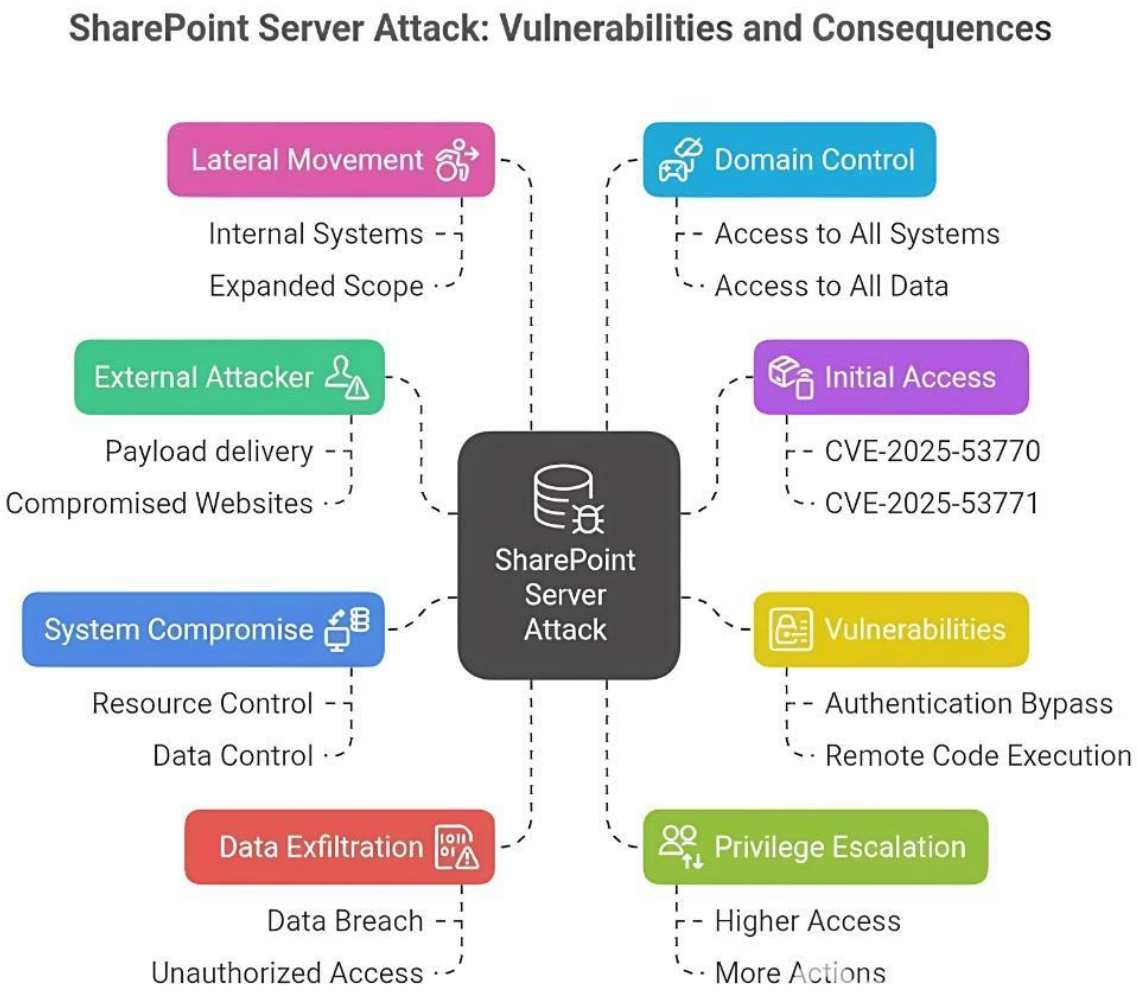
2. What Is the Threat?

CVE Details:

- CVE-2025-53770 (CVSS 9.8): Allows remote unauthenticated attackers to bypass authentication and execute arbitrary code via crafted requests to the ToolPane.aspx SharePoint component.
- CVE-2025-53771: Enables threat actors to exploit internal logic flaws and achieve post-authentication persistence.

The Exploit – “ToolShell”:

- A sophisticated attack chain named ToolShell is being used to deploy .aspx web shells (like spinstall0.aspx) on vulnerable servers.
- The attackers extract ASP.NET MachineKeys, allowing them to sign malicious payloads and evade detection.
- These payloads are capable of executing system commands, installing malware, and maintaining backdoors even after an apparent cleanup.



3. Global Campaign Status (As of July 22, 2025)

- Scope of Attack: Over 400 known compromised organizations, including the U.S. Department of Energy, National Institutes of Health (NIH), and other critical infrastructure.
- Threat Actors: The campaign is linked to China-based groups:
  - Linen Typhoon (APT27) – espionage-focused.
  - Violet Typhoon (APT31) – long-term persistent access.
  - Storm-2603 – ransomware deployment and destructive attacks.
- Exploitation Timeline:

- First waves began July 7, 2025.
- Coordinated attacks observed on July 18–19, 2025, showing rapid weaponization.

4. You might be vulnerable if:

- Suspicious POST requests to:/_layouts/15/ToolPane.aspx?DisplayMode=Edit
- Presence of unauthorized .aspx files such as spinstall0.aspx
- Unexpected changes to machineKey values in web.config
- Disabled antivirus or unexpected scheduled tasks
- Outbound connections to rare IPs or command-and-control domains

If this vulnerability is successfully exploited, it could lead to:

- Full takeover of your SharePoint server
- Credential theft and privilege escalation
- Deployment of ransomware
- Data exfiltration or service disruption

5. Indicators of Compromise (IOCs) & Tactics Observed

File Artifacts:

- Web shells: spinstall0.aspx, default.aspx, shell.aspx in C:\inetpub\wwwroot\wss\VirtualDirectories*

Web Logs:

- POST requests to:
  - /_layouts/15/ToolPane.aspx?DisplayMode=Edit
  - Headers with Referer: /_layouts/15/SignOut.aspx

System Activity:

- IIS worker process (w3wp.exe) launching PowerShell or command shell instances
- Registry modifications disabling Microsoft Defender
- Scheduled tasks running .NET assemblies from unusual paths

Credential Abuse:

- Use of Mimikatz, LSASS memory dumps
- Lateral movement tools: PsExec, Impacket, WMI remote execution

6. Immediate Actions Required

1. Apply Microsoft's July 2025 security updates immediately to all SharePoint servers.
2. Rotate all ASP.NET MachineKey values to prevent unauthorized persistence via compromised keys.
3. Restart all IIS services after patching to invalidate any active web shell sessions and cryptographic keys.
4. Temporarily disconnect all internet-exposed SharePoint servers until they are fully patched and security assessed.
5. Conduct a full scan for Indicators of Compromise (IOCs) using both endpoint and network detection tools.
6. Enable Antimalware Scan Interface (AMSI), Microsoft Defender Antivirus, and Microsoft Defender for Endpoint to improve detection of obfuscated and script-based threats.

7. Our Recommended Response Plan

We propose the following phased response to secure your environment:

Phase	Task
Assessment	Perform vulnerability scan + IOC hunt
Remediation	Patch, rotate keys, remove persistence
Threat Hunting	Analyze logs for any lateral movement or data theft
Hardening	Apply secure configuration baselines and least-privilege controls
Documentation	Prepare incident report and mitigation checklist

8.Conclusion

If your environment runs vulnerable, unpatched, or exposed Microsoft SharePoint servers, you must assume compromise is possible or underway. Given the scale and speed of these global exploitation campaigns, proactive steps must be taken immediately to ensure your environment is secure and monitored.

References:

- Microsoft Security Blog: https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/
- Microsoft Patch Guidance: https://msrc.microsoft.com/blog/2025/07/customer-guidance-for-sharepoint-vulnerability-cve-2025-53770/
- CISA Alert: https://www.cisa.gov/news-events/alerts/2025/07/20/update-microsoft-releases-guidance-exploitation-sharepoint-vulnerabilities/
- CSA Singapore Advisory: https://www.csa.gov.sg/alerts-and-advisories/advisories/ad-2025-016/

MODULAR AI AGENT FRAMEWORK FOR PROACTIVE THREAT DEFENSE AND CYBERCRIME RESPONSE

SAPTANG™
Proactive Threat Defence

Saptang Labs Pvt. Ltd.
sales@saptanglabs.com
9th floor, MRC Nagar 1st Lane, MRC Nagar, RA Puram, Chennai, Tamil Nadu 600028
www.saptanglabs.com