NCA-37.072425 – National CERT Advisory – Critical Remote Code Execution Vulnerability in Microsoft SharePoint Server (CVE-2025-53770)

Introduction

A critical Remote Code Execution (RCE) vulnerability, CVE-2025-53770 (CVSS v3.1 score: 9.8), has been identified in on-premises Microsoft SharePoint Server, which is actively being exploited in large-scale campaigns. This zero-day flaw allows unauthenticated attackers to execute arbitrary code over the network by exploiting SharePoint's deserialization mechanism.

Immediate mitigation is critical, especially for environments where SharePoint Server is exposed to the internet or lacks endpoint detection and response capabilities.

Impact

Successful exploitation of CVE-2025-53770 can result in:

1. **Full system compromise** – Vulnerability allows unauthenticated attackers to execute code and potentially deploy web shells (spinstall0.aspx)
2. **Remote Code Execution (RCE)** – Execution of arbitrary code without authentication.
3. **Widespread targeting** – Many industries using on-prem SharePoint are likely affected; assume compromise if servers were internet-facing
4. **Persistent Unauthorized Access** – Theft of cryptographic keys allows sustained access.
5. **Privilege Escalation and Lateral Movement** – Use of stolen MachineKey enables attack propagation.
6. **Detection Evasion** – Malicious activity can mimic legitimate SharePoint operations.
7. **Mass Compromise Risk** – Already confirmed exploitation across critical sectors globally.

Threat Details

Vulnerability Overview

- **CVE ID:** CVE-2025-53770
- **Component Affected:** Microsoft SharePoint Server (On-Premises)
- **Vulnerability Type:** Deserialization of Untrusted Data
- **Attack Vector:** Remote (Unauthenticated)
- **Attack Complexity:** Low
- **Privileges Required:** None

- **User Interaction:** None
- **CVSS v3.1 Score:** 9.8 (Critical)
- **CWE ID:** CWE-502 – Deserialization of Untrusted Data

Technical Description

CVE-2025-53770 allows attackers to exploit SharePoint's deserialization logic to inject and execute arbitrary commands prior to authentication. By manipulating the HTTP Referer header in requests (notably involving `/_layouts/SignOut.aspx`), attackers can bypass earlier fixes for CVE-2025-49704 and CVE-2025-49706.

Once exploited, attackers gain access to SharePoint MachineKey configuration (`ValidationKey, DecryptionKey`), allowing them to craft forged `__VIEWSTATE` payloads that are trusted by the application. This enables stealthy post-exploitation activities, often via PowerShell and ASPX web shells.

This exploit chain is codenamed ToolShell, and is actively being used in the wild.

Exploit Conditions

To exploit this vulnerability:

- The target is an on-premises Microsoft SharePoint Server.
- AMSI integration is not enabled (enabled by default only in newer updates).
- The server is internet-exposed or accessible over an internal network.
- No endpoint protection or behavioral monitoring is in place.
- In many cases, no authentication is required for initial access.

Affected Systems & Required Updates

Product	Impacted Versions	Fixed Version	Action Required
Microsoft SharePoint Server (2016/2019/Subscription Edition)	All on-premise installations not patched after July 19, 2025	Patch issued July 21, 2025	Apply latest security update immediately

Recommendations & Mitigation Actions

1. Patch Immediately (Preferred Fix)

- Apply the patch that addresses CVE-2025-53770 and CVE-2025-53771.

- Restart affected services post-patch and confirm the integrity of cryptographic keys.

2. Enable AMSI Integration

- Ensure Antimalware Scan Interface (AMSI) is enabled in SharePoint.
- This is enabled by default in:
  - SharePoint Server 2016/2019 (September 2023 Update)
  - Subscription Edition (Version 23H2+)

3. Deploy Defender AV and Defender for Endpoint

- Ensure Microsoft Defender Antivirus is installed and updated.
- Deploy Defender for Endpoint to monitor lateral movement and post-exploitation behaviors.

4. Isolate SharePoint Servers Temporarily

- If patching is not feasible, disconnect vulnerable SharePoint servers from the internet.
- Apply strict firewall rules and network segmentation.

5. Reset Cryptographic Keys Post-Patch

- Rotate MachineKey settings to invalidate stolen tokens or payloads.
- Regenerate ValidationKey and DecryptionKey in web.config.

6. Enable ATC Advance Threat Control

- Ensure Advanced Threat Control (ATC) is enabled to block zero-day attacks by monitoring

Monitoring & Detection

- Monitor for unusual activity in:
  - `__VIEWSTATE` manipulation
  - `ToolPane.aspx` and `SignOut.aspx` HTTP Referer headers
  - PowerShell or ASPX file deployment on SharePoint directories
- Use EDR and SIEM tools to detect:
  - Web shell behavior and persistent backdoors
  - Lateral movement originating from SharePoint hosts

- Unauthorized access or configuration changes

Incident Response & Readiness

- Update IR playbooks to include ToolShell exploitation scenarios.
- Conduct threat hunting for compromised cryptographic keys.
- Validate the integrity and security of SharePoint backups.
- Perform red-team simulations simulating MachineKey theft and web shell persistence.

Patching Summary

Product	Version Range	Status	Action
Microsoft SharePoint Server	Unpatched pre-July 20, 2025	Vulnerable	Apply patch released July 20, 2025
Microsoft SharePoint Server	Patched (as of July 21, 2025)	Secure	No further action required (consider key rotation)

References

1. **Microsoft Security Advisory** – https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53770
2. **Customer guidance for SharePoint vulnerability CVE-2025-53770** – https://msrc.microsoft.com/blog/2025/07/customer-guidance-for-sharepoint-vulnerability-cve-2025-53770/
3. NIST NVD CVE Entry – https://nvd.nist.gov/vuln/detail/CVE-2025-53770
4. Tenable Security Advisory – https://www.tenable.com/cve/CVE-2025-53770

Call to Action

The National CERT advises all organizations using on-premise Microsoft SharePoint Server to:

- Apply the security patch issued July 20, 2025, without delay.
- Rotate cryptographic keys post-patch to prevent unauthorized reuse.
- Implement endpoint monitoring and deploy Microsoft Defender solutions.
- Isolate vulnerable servers until patched and verified.

Swift patching and layered detection controls are essential to prevent persistent unauthorized access and wide-scale exploitation.