CyRisk

URGENT SECURITY UPDATE BULLETIN

Critical SharePoint Vulnerability (CVE-2025-53770)

We are issuing an urgent alert regarding a critical and actively exploited vulnerability, identified as CVE-2025-53770, affecting on-premises Microsoft SharePoint Servers. This vulnerability, which Microsoft has confirmed is being actively exploited in the wild, allows unauthorized attackers to execute code remotely on vulnerable servers without needing to authenticate. The risk is significant: attackers can gain full control over your SharePoint servers, bypass existing identity protections like Multi-Factor Authentication (MFA) or Single Sign-On (SSO), access all SharePoint content, file systems, and internal configurations, and potentially move laterally across your Windows Domain. Of particular concern is the theft of cryptographic keys, which allows attackers to impersonate users or services even after a server has been patched, meaning patching alone is not sufficient for full remediation.

Please note: **SharePoint Online in Microsoft 365 is not impacted** by these vulnerabilities.

If you would like assistance with this vulnerability or want to discuss other security issues, please click on this link to schedule a call with one of our experienced security professionals.

TECHNICAL GUIDANCE

1. Background on the Vulnerability:

- CVE-2025-53770 is a deserialization of untrusted data vulnerability in on-premises Microsoft SharePoint Server. It is a variant of CVE-2025-49704, and exists as part of a chain of vulnerabilities, publicly reported as "ToolShell," which also includes CVE-2025-53771 (a patch bypass for CVE-2025-49706, a network spoofing vulnerability).
- The exploit leverages a specific HTTP Referrer header (/_layouts/SignOut.aspx) to bypass authentication when interacting with /_layouts/15/ToolPane.aspx, allowing attackers to write files to the server without authentication.
- The initial payload often drops a stealthy spinstall0.aspx file, which extracts and leaks cryptographic secrets, specifically the SharePoint server's ASP.NET MachineKey configuration, including the ValidationKey.
- Once the cryptographic material (ValidationKey) is leaked, attackers can craft valid, signed __VIEWSTATE payloads using tools like ysoserial to execute arbitrary commands remotely, completing the Remote Code Execution (RCE) chain without requiring credentials.

2. How to Detect if Your System is Vulnerable:

Microsoft Defender Detections:

- **Microsoft Defender Antivirus** provides detection and protection under the names: Exploit:Script/SuspSignoutReq.A and Trojan:Win32/HijackSharePointServer.A.
- **Microsoft Defender for Endpoint** alerts may indicate threat activity with titles such as: "Possible web shell installation," "Possible exploitation of SharePoint server vulnerabilities," "Suspicious IIS worker process behavior," "IIS worker process loaded suspicious .NET assembly," and blocked

malware alerts like "SuspSignoutReq malware was blocked on a SharePoint server" or "HijackSharePointServer malware was blocked on a SharePoint server".

- **Microsoft Defender Vulnerability Management (MDVM)** includes vulnerability records with CVSS scores and zero-day flags for both CVE-2025-53770 and CVE-2025-53771 for all impacted SharePoint versions. You can browse to Vulnerability management -> Software vulnerabilities and filter by these CVE identifiers to view exposed devices, remediation status, and Evidence of Exploitation tags.

Advanced Hunting Queries (Microsoft 365 Defender):

- **Unified Advanced Hunting Query:** DeviceTvmSoftwareVulnerabilities | where CveId in ("CVE-2025-49706", "CVE-2025-53770").
- **Successful exploitation via file creation (requires Microsoft 365 Defender):** Look for the creation of spinstall0.aspx in SharePoint layouts paths: DeviceFileEvents | where FolderPath has_any ('microsoft shared\Web Server Extensions\16\TEMPLATE\LAYOUTS', 'microsoft shared\Web Server Extensions\15\TEMPLATE\LAYOUTS') | where FileName has "spinstall0" | project Timestamp, DeviceName, InitiatingProcessFileName, InitiatingProcessCommandLine, FileName, FolderPath, ReportId, ActionType, SHA256 | order by Timestamp desc.
- **Process Creation (w3wp.exe spawning encoded PowerShell):** Look for w3wp.exe spawning encoded PowerShell involving the spinstall0 file or its known file paths: DeviceProcessEvents | where InitiatingProcessFileName has "w3wp.exe" and InitiatingProcessCommandLine !has "DefaultAppPool" and FileName =~ "cmd.exe" and ProcessCommandLine has_all ("cmd.exe", "powershell") and ProcessCommandLine has_any ("EncodedCommand", "-ec") | extend CommandArguments = split(ProcessCommandLine, " ") | mv-expand CommandArguments to typeof(string) | where CommandArguments matches regex "^[A-Za-z0-9+/=]{15,}$" | extend B64Decode = replace("\\x00", "", base64_decodestring(tostring(CommandArguments))) | where B64Decode has_any ("spinstall0",
'C:\PROGRA~1\COMMON~1\MICROS~1\WEBSER~1\15\TEMPLATE\LAYOUTS',
'C:\PROGRA~1\COMMON~1\MICROS~1\WEBSER~1\16\TEMPLATE\LAYOUTS').

Indicators of Compromise (IOCs):

- **Malicious Files:** Look for spinstall0.aspx (or variants like spinstall.aspx, spinstall1.aspx, spinstall2.aspx) in the following locations:
  - 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.
  - SHA256 hash of the spinstall0.aspx crypto dumper: **92bb4ddb98eeaf11fc15bb32e71d0a63256a0ed826a03ba293ce3a8bf057a514**.
- **HTTP Requests & Logs:**
  - Monitor for **POST requests to /_layouts/15/ToolPane.aspx?DisplayMode=Edit**.

- Look for the specific user agent string used in active exploitation: **Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101 Firefox/120.0** or its encoded form in IIS logs.
- Check for the exact HTTP Referer header used: **Referer: /_layouts/SignOut.aspx** (or full URI Referers like https://<target>/_layouts/SignOut.aspx or http://<target>/_layouts/SignOut.aspx).

- **Malicious IP Addresses (Exploit Waves):** Conduct scanning for connections to/from these IPs, especially between July 18-19, 2025:
  - 107.191.58[.]76 (first exploit wave).
  - 104.238.159[.]149 (second exploit wave).
  - 96.9.125[.]147 (initial exploit wave).
  - Additional IPs for later waves (on and after July 21): 45.191.66[.]77, 45.77.155[.]170, 64.176.50[.]109, 206.166.251[.]228, 34.72.225[.]196, 34.121.207[.]116, 141.164.60[.]10, 134.199.202[.]205, 188.130.206[.]168.
  - Post-exploitation C2 traffic: 131.226.2[.]6.

3. What to Do If Your System is Vulnerable (Immediate Response Recommendations):

- **Isolate or Shut Down:** Immediately **isolate or shut down affected SharePoint servers**. Blocking via firewall alone is not enough, as persistence may already exist.
- **Renew Credentials and Secrets: Renew all credentials and system secrets** that could have been exposed via the malicious ASPX file.
- **Engage Incident Response: Engage your incident response team or a trusted cybersecurity firm** immediately. Time is critical.
- **Decommission End-of-Life Servers:** Disconnect public-facing versions of SharePoint Server that have reached their End-of-Life (EOL) or End-of-Service (EOS), such as SharePoint Server 2013 and earlier versions, from the internet. **No patch is expected for these older versions**.

4. How to Patch and Mitigate the Risks:

- **Apply Latest Security Updates Immediately:** Microsoft has released security updates that fully protect supported versions of SharePoint affected by CVE-2025-53770 and CVE-2025-53771. These updates are cumulative, so applying the latest one will include earlier fixes.
  - **Microsoft SharePoint Server Subscription Edition:** Download Security Update for Microsoft SharePoint Server Subscription Edition (KB5002768).
  - **Microsoft SharePoint Server 2019:** Download Security Update for Microsoft SharePoint 2019 (KB5002754) and Security Update for Microsoft SharePoint Server 2019 Language Pack (KB5002753).
  - **Microsoft SharePoint Server 2016:** Security Update for Microsoft SharePoint Enterprise Server 2016 (KB5002760) and Security Update for Microsoft SharePoint Enterprise Server 2016 Language Pack (KB5002759).

  - **Ensure you are using supported versions of on-premises SharePoint Server** (2016, 2019, & Subscription Edition).

- **Rotate SharePoint Server ASP.NET Machine Keys:**
  - **This is a CRITICAL step** after applying the latest security updates or enabling AMSI. Patching alone is not enough to invalidate previously stolen cryptographic material.
  - **After rotation, restart IIS on all SharePoint servers** using iisreset.exe.
  - **PowerShell Guidance for Machine Key Rotation:**
    - Generate the machine key: Set-SPMachineKey -WebApplication <SPWebApplicationPipeBind>.
    - Deploy the machine key to the farm: Update-SPMachineKey -WebApplication <SPWebApplicationPipeBind>.
    - For bulk rotation (use with caution): Get-SPWebApplication | ForEach-Object { Write-Host "Updating machine key for $($_.Url)"; Set-SPMachineKey -WebApplication $_; Update-SPMachineKey -WebApplication $_ }.
    - Note that in clustered or load-balanced environments, specialized consultation may be required.
- **Deploy Microsoft Defender for Endpoint (or Equivalent Threat Solutions):** We recommend deploying Defender for Endpoint to detect and block post-exploit activity.
- **Ensure the Antimalware Scan Interface (AMSI) is Turned On and Configured Correctly:**
  - Configure AMSI integration in SharePoint. If HTTP Request Body scanning is available, **enable Full Mode** for the most comprehensive protection.
  - Deploy **Microsoft Defender Antivirus** on all SharePoint servers, as this will stop unauthenticated attackers from exploiting this vulnerability.
  - AMSI integration was enabled by default in the September 2023 security update for SharePoint Server 2016/2019 and the Version 23H2 feature update for SharePoint Server Subscription Edition.
  - If you cannot enable AMSI, consider disconnecting your server from the Internet until updates are applied, or use a VPN or proxy requiring authentication to limit unauthenticated traffic.
- **Additional Security Measures:**
  - Update intrusion prevention system and web-application firewall (WAF) rules to block exploit patterns and anomalous behavior.
  - Implement comprehensive logging to identify exploitation activity.
  - Audit and minimize layout and admin privileges.