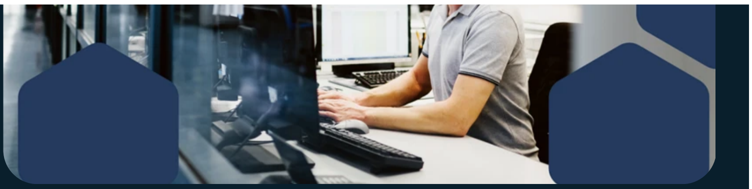
Research • July 22 • 11 min read

Disrupting active exploitation of

on-premises SharePoint vulnerabilities



By Microsoft Threat Intelligence

CVE-2025-49706, a spoofing vulnerability, and CVE-2025-49704, a remote code execution vulnerability. These vulnerabilities affect on-premises SharePoint servers only and do not affect SharePoint Online in Microsoft 365. Microsoft has released new comprehensive security updates for all supported versions of SharePoint Server (Subscription Edition, 2019, and 2016) that protect customers against these new vulnerabilities. Customers should apply these updates immediately to ensure they are protected.

These comprehensive security updates address newly disclosed security vulnerabilities in CVE-2025-53770 that are related to the previously disclosed vulnerability CVE-2025-49704. The updates also address the security bypass vulnerability CVE-2025-53771 for the previously disclosed CVE-2025-49706.

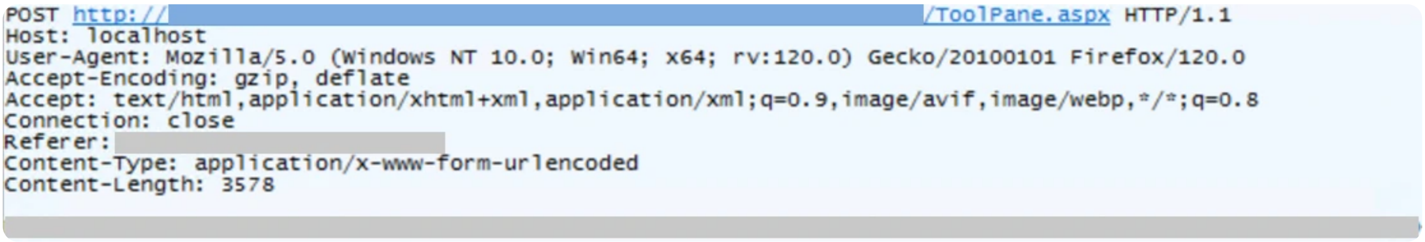
As of this writing, Microsoft has observed two named Chinese nation-state actors, Linen Typhoon and Violet Typhoon exploiting these vulnerabilities targeting internet-facing SharePoint servers. In addition, we have observed another China-based threat actor, tracked as Storm-2603, exploiting these vulnerabilities. Investigations into other actors also using these exploits are still ongoing. With the rapid adoption of these exploits, Microsoft assesses with high confidence that threat actors will continue to integrate them into their attacks against unpatched on-premises SharePoint systems. This blog shares details of observed exploitation of CVE-2025-49706 and CVE-2025-49704 and the follow-on tactics, techniques, and procedures (TTPs) by threat actors. We will update this blog with more information as our investigation continues.

Microsoft recommends customers to use supported versions of on-premises SharePoint servers with the latest security updates. To stop unauthenticated attacks from exploiting this vulnerability, customers should also integrate and enable Antimalware Scan Interface (AMSI) and Microsoft Defender Antivirus (or equivalent solutions) for all on-premises SharePoint deployments and configure AMSI to enable Full Mode as detailed in Mitigations section below. Customers should also rotate SharePoint server ASP.NET machine keys, restart Internet Information Services (IIS), and deploy Microsoft Defender for Endpoint or equivalent solutions.

Product	Security update link
Microsoft SharePoint Server Subscription Edition	Security Update for Microsoft SharePoint Server Subscription Edition (KB5002768)
Microsoft SharePoint Server 2019 *(both updates should be installed)*	Security Update for Microsoft SharePoint 2019 (KB5002754) Security Update for Microsoft SharePoint Server 2019 Language Pack (KB5002753)
Microsoft SharePoint Server 2016 *(both updates should be installed)*	Security Update for Microsoft SharePoint Enterprise Server 2016 (KB5002760) Security Update for Microsoft SharePoint Enterprise Server 2016 Language Pack (KB5002759)

Observed tactics and techniques

Microsoft observed multiple threat actors conducting reconnaissance and attempting exploitation of on-premises SharePoint servers through a POST request to the ToolPane endpoint.



```
POST http://[redacted]/ToolPane.aspx HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101 Firefox/120.0
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Connection: close
Referer: [redacted]
Content-Type: application/x-www-form-urlencoded
Content-Length: 3578
```

Figure 1. POST request to ToolPane endpoint

Post-exploitation activities

Threat actors who successfully executed the authentication bypass and remote code execution exploits against vulnerable on-premises SharePoint servers have been observed using a web shell in their post-exploitation payload.

Web shell deployment

In observed attacks, threat actors send a crafted POST request to the SharePoint server, uploading a malicious script named *spinstall0.aspx*. Actors have also modified the file name in a variety of ways, such as *spinstall.aspx*, *spinstall1.aspx*, *spinstall2.aspx*, etc. The *spinstall0.aspx* script contains commands to retrieve MachineKey data and return the results to the user through a GET request, enabling the theft of the key material by threat actors.

Related IOCs and hunting queries

Microsoft provides indicators of compromise (IOCs) to identify and hunt for this web shell in the Indicators of compromise section of this blog. Microsoft provides related hunting queries to find this dropped file in the Hunting queries section of this blog.

Attribution

As early as July 7, 2025, Microsoft analysis suggests threat actors were attempting to exploit CVE-2025-49706 and CVE-2025-49704 to gain initial access to target organizations. These actors include Chinese state actors Linen Typhoon and Violet Typhoon and another China-based actor Storm-2603. The TTPs employed in these exploit attacks align with previously observed activities of these threat actors.

Linen Typhoon

Since 2012, Linen Typhoon has focused on stealing intellectual property, primarily targeting organizations related to government, defense, strategic planning, and human rights. This threat actor is known for using drive-by compromises and historically has relied on existing exploits to compromise organizations.

Violet Typhoon

Since 2015, the Violet Typhoon activity group has been dedicated to espionage, primarily targeting former government and military personnel, non-governmental organizations (NGOs), think tanks, higher education, digital and print media, financial and health related sectors in the United States, Europe, and East Asia. This group persistently scans for vulnerabilities in the exposed web infrastructure of target organizations, exploiting discovered weaknesses to install web shells.

Storm-2603

The group Microsoft tracks as Storm-2603 is assessed with medium confidence to be a China-based threat actor. Microsoft has not identified links between

Storm-2603 and other known Chinese threat actors. Microsoft tracks this threat actor in association with attempts to steal MachineKeys via the on-premises SharePoint vulnerabilities. Although Microsoft has observed this threat actor deploying Warlock and Lockbit ransomware in the past, Microsoft is currently unable to confidently assess the threat actor’s objectives.

Additional actors may use these exploits to target unpatched on-premises SharePoint systems, further emphasizing the need for organizations to implement mitigations and security updates immediately.

Mitigation and protection guidance

Microsoft has released security updates that fully protect customers using all supported versions of SharePoint affected by CVE-2025-53770 and CVE-2025-53771. Customers should apply these updates immediately.

Customers using SharePoint Server should follow the guidance below.

1. **Use or upgrade to supported versions of on-premises Microsoft SharePoint Server.**
    - Supported versions: SharePoint Server 2016, 2019, and SharePoint Subscription Edition
2. **Apply the latest security updates.**
3. **Ensure the Antimalware Scan Interface is turned on and configured correctly and deploy Defender Antivirus on all SharePoint servers**
    - Configure Antimalware Scan Interface (AMSI) integration in SharePoint, enable Full Mode for optimal protection, and deploy Defender Antivirus on all SharePoint servers which will stop unauthenticated attackers from exploiting this vulnerability.
    - Note: 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, we recommend you consider disconnecting your server from the internet until you have applied the

    most current security update linked above. If the server cannot be disconnected from the internet, consider using a VPN or proxy requiring authentication or an authentication gateway to limit unauthenticated traffic.

4. **Deploy Microsoft Defender for Endpoint, or equivalent solutions**
    - We recommend organizations to deploy Defender for Endpoint to detect and block post-exploit activity.
5. **Rotate SharePoint Server ASP.NET machine keys**
    - After applying the latest security updates above or enabling AMSI, it is critical that customers rotate SharePoint server ASP.NET machine keys and restart Internet Information Services (IIS) on all SharePoint servers.
        1. Manually via PowerShell
            - To update the machine keys using PowerShell, use the Set-SPMachineKey cmdlet.
        2. Manually via Central Admin: Trigger the Machine Key Rotation timer job by performing the following steps:
            - Navigate to the **Central Administration** site.
            - Go to **Monitoring** -> **Review job definition**.
            - Search for **Machine Key Rotation Job** and select **Run Now**.
    - After the rotation has completed, restart IIS on all SharePoint servers using *iisreset.exe*.
    - NOTE: If you cannot enable AMSI, you will need to rotate your keys after you install the new security update.

Indicators of compromise

Indicator	Type	Description
Spinstall0.aspx	File name	Web shell used by threat actors Actors have also modified the file name in a variety of ways, such as *spinstall.aspx*, *spinstall1.aspx*, *spinstall2.aspx*

debug_dev.js	File name	File containing web config data, including MachineKey data
92bb4ddb98eeaf11fc15bb32e71d0a63256a0ed826a03ba293ce3a8bf057a514	SHA-256	Hash of *spinstall0.aspx*
c34718cbb4c6.ngrok-free[.]app/file.ps1	URL	Ngrok tunnel delivering PowerShell to C2
\1[5-6]\TEMPLATE\LAYOUTS\debug_dev.js	File path	File path for stolen web configs
131.226.2[.]6	IP	Post exploitation C2
134.199.202[.]205	IP	IP address exploiting SharePoint vulnerabilities
104.238.159[.]149	IP	IP address exploiting SharePoint vulnerabilities
188.130.206[.]168	IP	IP address exploiting SharePoint vulnerabilities

Microsoft Defender XDR coverage

Microsoft Defender XDR customers get coordinated protection across endpoints, identities, email, and cloud apps to detect, prevent, investigate, and respond to threats like the SharePoint exploitation activity described in this blog.

Customers with provisioned access can also use Microsoft Security Copilot in Microsoft Defender to investigate and respond to incidents, hunt for threats, and protect their organization with relevant threat intelligence.

The following table outlines the tactics observed in the exploitation attacks discussed in this blog, along with Microsoft Defender protection coverage at each stage of the attack chain:

Tactic	Observed activity	Microsoft Defender coverage
Initial access	Use of known vulnerabilities to exploit internet-facing SharePoint servers	**Microsoft Defender Antivirus** – Exploit:Script/SuspSignoutReq.A – Exploit:Script/SuspSignoutReqBody.A **Microsoft Defender for Endpoint** – 'SuspSignoutReq' malware was blocked on a SharePoint server – Possible exploitation of SharePoint server vulnerabilities
Execution	PowerShell script execution used to launch payloads	**Microsoft Defender Antivirus** – Trojan:Win32/HijackSharePointServer.A **Microsoft Defender for Endpoint** – Suspicious IIS worker process behavior
Persistence	Web shell used to steal machine keys and persist access	**Microsoft Defender Antivirus** – Trojan:PowerShell/MachineKeyFinder.DA!amsi **Microsoft Defender for Endpoint** – Possible web shell installation
Defense evasion	Payload reflectively loaded via IIS process	**Microsoft Defender for Endpoint** – IIS worker process loaded suspicious .NET assembly
Collection	Web shell used to extract MachineKey data	**Microsoft Defender Antivirus** – Trojan:PowerShell/MachineKeyFinder.DA!amsi **Microsoft Defender for Endpoint** – Possible web shell installation

Note: These alerts can also be triggered by unrelated threat activity

Vulnerability management

Customers using Microsoft Defender Vulnerability Management can identify exposed devices and track remediation efforts based on the following CVEs:

- CVE-2025-53770 – SharePoint ToolShell Auth Bypass and RCE
- CVE-2025-53771 – SharePoint ToolShell Path Traversal
- CVE-2025-49704 – SharePoint RCE
- CVE-2025-49706 – SharePoint Post-auth RCE

Navigate to **Vulnerability management** > **Software vulnerabilities**, filter by CVE, and look for **Evidence of Exploitation** tags for affected assets.

External Attack Surface Management (Defender EASM)

Microsoft Defender External Attack Surface Management (Defender EASM) provides visibility into exposed internet-facing SharePoint instances. The following Attack Surface Insights may indicate vulnerable but not necessarily exploited services:

- CVE-2025-49704 – SharePoint RCE
- CVE-2025-53770 – SharePoint ToolShell Auth Bypass and RCE
- CVE-2025-53771 – SharePoint ToolShell Path Traversal

Note: A “Potential” insight signals that a service is detected but version validation is not possible. Customers should manually verify patching status.

Hunting queries

Microsoft Defender XDR

To locate possible exploitation activity, run the following queries in Microsoft Defender XDR security center.

Successful exploitation via file creation

Look for the creation of *spinstall0.aspx*, which indicates successful post-exploitation of CVE-2025-53770.

```
DeviceFileEvents
| where FolderPath has_any ("microsoft shared\\Web Server Extensions\\15\\TEMPLATE
| where FileName contains "spinstall"
| project Timestamp, DeviceName, InitiatingProcessFileName, InitiatingProcessComma
| order by Timestamp desc
```

Post-exploitation PowerShell dropping web shell

Look for process creation where *w3wp.exe* is spawning encoded PowerShell involving the *spinstall0.aspx* file or the file paths it's been known to be written to.

```
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(CommandArgu
| where B64Decode contains "spinstall", @'C:\PROGRA~1\COMMON~1\MICROS~1\WEBSER~1\1
```

Post-exploitation web shell dropped

Look for the web shell dropped via the PowerShell command.

```
DeviceFileEvents
| where Timestamp >ago(7d)
| where InitiatingProcessFileName=~"powershell.exe"
| where FileName contains "spinstall"
```

Exploitation detected by Defender

Look at Microsoft Defender for Endpoint telemetry to determine if specific alerts fired in your environment.

```
AlertEvidence
| where Timestamp > ago(7d)
| where Title has "SuspSignoutReq"
| extend _DeviceKey = iff(isnotempty(DeviceId), bag_pack_columns(DeviceId, DeviceN
| summarize min(Timestamp), max(Timestamp), count_distinctif(DeviceId,isnotempty(D
```

Unified advanced hunting queries

Find exposed devices

Look for devices vulnerable to the CVEs listed in blog.

```
DeviceTvmSoftwareVulnerabilities
| where CveId in ("CVE-2025-49704","CVE-2025-49706","CVE-2025-53770","CVE-2025-537
```

Microsoft Sentinel

Microsoft Sentinel customers can use the TI Mapping analytics (a series of analytics all prefixed with 'TI map') to automatically match the malicious domain indicators mentioned in this blog post with data in their workspace. If the TI Map analytics are not currently deployed, customers can install the Threat Intelligence solution from the Microsoft Sentinel Content Hub to have the analytics rule deployed in their Sentinel workspace.

Our post on web shell threat hunting with Microsoft Sentinel also provides guidance on looking for web shells in general. Several hunting queries are also available below:

- Web shell detection
- Possible Webshell drop
- Malicious web application requests linked with Microsoft Defender for Endpoint alerts
- Web shell activity

Below are the queries using Sentinel Advanced Security Information Model (ASIM) functions to hunt threats across both Microsoft first-party and third-party data sources. ASIM also supports deploying parsers to specific workspaces from GitHub, using an ARM template or manually.

Detect network indicators of compromise and file hashes via ASIM

```
//IP list and domain list- _Im_NetworkSession
let lookback = 30d;
let ioc_ip_addr = dynamic(["131.226.2.6", "134.199.202.205", "104.238.159.149", "1
let ioc_domains = dynamic(["c34718cbb4c6.ngrok-free.app"]);
_Im_NetworkSession(starttime=todatetime(ago(lookback)), endtime=now())
| where DstIpAddr in (ioc_ip_addr) or DstDomain has_any (ioc_domains)
| summarize imNWS_mintime=min(TimeGenerated), imNWS_maxtime=max(TimeGenerated),
  EventCount=count() by SrcIpAddr, DstIpAddr, DstDomain, Dvc, EventProduct, EventV


//IP list - _Im_WebSession
let lookback = 30d;
let ioc_ip_addr = dynamic(["131.226.2.6", "134.199.202.205", "104.238.159.149", "1
let ioc_sha_hashes =dynamic(["92bb4ddb98eeaf11fc15bb32e71d0a63256a0ed826a03ba293ce
_Im_WebSession(starttime=todatetime(ago(lookback)), endtime=now())
| where DstIpAddr in (ioc_ip_addr) or FileSHA256 in (ioc_sha_hashes)
| summarize imWS_mintime=min(TimeGenerated), imWS_maxtime=max(TimeGenerated),
  EventCount=count() by SrcIpAddr, DstIpAddr, Url, Dvc, EventProduct, EventVendor


// file hash list - imFileEvent
let ioc_sha_hashes = dynamic(["92bb4ddb98eeaf11fc15bb32e71d0a63256a0ed826a03ba293c
imFileEvent
| where SrcFileSHA256 in (ioc_sha_hashes) or TargetFileSHA256 in (ioc_sha_hashes)
| extend AccountName = tostring(split(User, @'')[1]),
  AccountNTDomain = tostring(split(User, @'')[0])
| extend AlgorithmType = "SHA256"
```

Microsoft Security Copilot

Microsoft Security Copilot customers can use the standalone experience to create their own prompts or run the following prebuilt promptbooks to automate incident response or investigation tasks related to this threat:

- Vulnerability impact assessment

Note that some promptbooks require access to plugins for Microsoft products such as Microsoft Defender XDR or Microsoft Sentinel.

Threat intelligence reports

Microsoft customers can use the following reports in Microsoft products to get the most up-to-date information about the threat actor, malicious activity, and techniques discussed in this blog. These reports provide the intelligence, protection information, and recommended actions to prevent, mitigate, or respond to associated threats found in customer environments.

Microsoft Defender Threat Intelligence

- CVE-2025-53770 – Microsoft SharePoint server remote code execution vulnerability

Microsoft Security Copilot customers can also use the Microsoft Security Copilot integration in Microsoft Defender Threat Intelligence, either in the Security Copilot standalone portal or in the embedded experience in the Microsoft Defender portal to get more information about this threat actor.

MITRE ATT&CK techniques observed

Threat actors have exhibited use of the following attack techniques. For standard industry documentation about these techniques, refer to the MITRE ATT&CK framework.

Initial Access

- T1190 Exploit public-facing application | Use of known vulnerabilities to exploit internet facing on-premises SharePoint severs

Execution

- T1059.001 Command and scripting interpreter: PowerShell | Use of a web shell to run PowerShell to read and transmit MachineKey data to attacker

Persistence

- T1505.003 Server software component: web shell | Threat actors install web shell after exploiting SharePoint vulnerability

Defense Evasion

- T1620 Reflective code loading | Reflectively loaded payloads

Collection

- T1119 Automated collection | Use of web shell to display MachineKey data

References

- CodeWhiteSec POC (X)
- Khoa Dinh POC (X)
- CVE-2025-53770 (MSRC)
- CVE-2025-49704 (MSRC
- CVE-2025-49706 (MSRC
- CVE-2025-53771 (MSRC)

Learn more

Meet the experts behind Microsoft Threat Intelligence, Incident Response, and the Microsoft Security Response Center at our VIP Mixer at Black Hat 2025. Discover how our end-to-end platform can help you strengthen resilience and elevate your security posture.

For the latest security research from the Microsoft Threat Intelligence community, check out the Microsoft Threat Intelligence Blog.

To get notified about new publications and to join discussions on social media, follow us on LinkedIn, X (formerly Twitter), and Bluesky.

To hear stories and insights from the Microsoft Threat Intelligence community about the ever-evolving threat landscape, listen to the Microsoft Threat Intelligence podcast.

Microsoft Threat Intelligence

See Microsoft Threat Intelligence posts

Related posts

Get started with Microsoft Security

Protect your people, data, and infrastructure with AI-powered, end-to-end security from Microsoft.

Learn how

Connect with us on social

What's new

- Surface Pro
- Surface Laptop
- Surface Laptop Studio 2
- Surface Laptop Go 3
- Microsoft Copilot
- AI in Windows
- Explore Microsoft

Microsoft Store

- Account profile
- Download Center
- Microsoft Store support
- Returns
- Order tracking
- Certified Refurbished

Education

- Microsoft in education
- Devices for education
- Microsoft Teams for Education
- Microsoft 365 Education
- How to buy for your school

Business

- Microsoft Cloud
- Microsoft Security
- Dynamics 365
- Microsoft 365
- Microsoft Power Platform
- Microsoft Teams
- Microsoft 365 Copilot

Developer & IT

- Azure
- Microsoft Developer
- Microsoft Learn
- Support for AI marketplace apps
- Microsoft Tech Community

Company

- Careers
- About Microsoft
- Company news
- Privacy at Microsoft
- Investors
- Diversity and inclusion
- Accessibility

products

Windows 11 apps

Microsoft Store Promise

Flexible Payments

Educator training and development

Deals for students and parents

AI for education

Small Business

Azure Marketplace

AppSource

Visual Studio

Sustainability

English (United States)

Your Privacy Choices

Consumer Health Privacy

Sitemap

Contact Microsoft

Privacy

Manage cookies

Terms of use

Trademarks

Safety & eco

Recycling

About our ads