Author: Jack Fitzgerald

Official Incident Report

Date: Jul, 22, 2025, 01:07 PM

Event ID: 320

Rule Name: SOC342 - CVE-2025-53770 SharePoint ToolShell Auth Bypass and RCE

Table of Contents

Alert Details

Severity: Critical

Type: Web Attack

Hostname: SharePoint01

Source IP Address: 107.191.58.76

Destination IP Address: 172.16.20.17

HTTP Request Method: POST

Requested URL: /_layouts/15/ToolPane.aspx?DisplayMode=Edit&a=/ToolPane.aspx

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101 Firefox/120.0

Referer: /_layouts/SignOut.aspx

Content-Length: 7699

Alert Trigger Reason: Suspicious unauthenticated POST request targeting ToolPane.aspx with large payload size and spoofed referer indicative of CVE-2025-53770 exploitation.

Device Action: Allowed

Based on the information provided in the alert, it appears the SIEM has detected behaviour linked to **CVE-2025-53770**, which could allow an **unauthorized attacker** to **execute code over a network** in an on-premises **Microsoft SharePoint Server**. The alert is triggered by rule SOC342 - CVE-2025-53770 SharePoint ToolShell Auth Bypass and RCE.

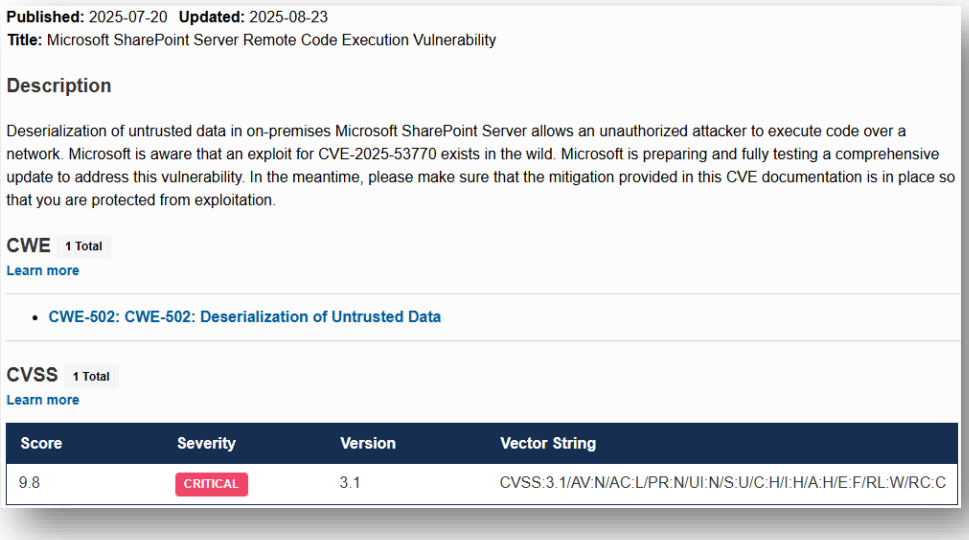
Overall, it appears that the **alert** may be suspicious, and further investigation is needed to identify the extent of the alert and determine if any necessary actions are required to remediate the situation.

Detection

Verify

As a security analyst, one of the first steps we take to verify the alert and determine whether it is a **false positive** or a **true positive** incident is to analyse the logs collected from the host by our security products.

A summary of CVE-2025-53770.



Published: 2025-07-20 **Updated:** 2025-08-23
Title: Microsoft SharePoint Server Remote Code Execution Vulnerability

Description

Deserialization of untrusted data in on-premises Microsoft SharePoint Server allows an unauthorized attacker to execute code over a network. Microsoft is aware that an exploit for CVE-2025-53770 exists in the wild. Microsoft is preparing and fully testing a comprehensive update to address this vulnerability. In the meantime, please make sure that the mitigation provided in this CVE documentation is in place so that you are protected from exploitation.

CWE 1 Total
Learn more

- CWE-502: CWE-502: Deserialization of Untrusted Data

CVSS 1 Total
Learn more

Score	Severity	Version	Vector String
9.8	CRITICAL	3.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:W/RC:C

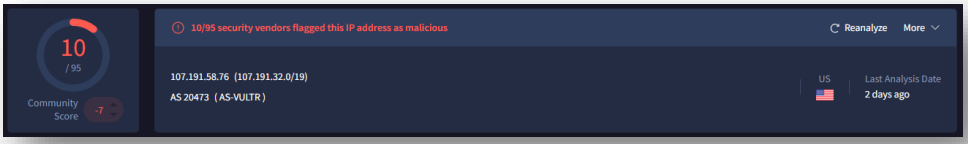
According to the Microsoft Security Blog, threat actors who successfully executed the authentication bypass and remote code execution exploits against vulnerable on-premises SharePoint servers have been observed using a **web shell** in their **post-exploitation payload**.

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.

The CVE summary tells us why the alert was triggered; however, we need to collect data related to the devices and traffic involved via our online tools.

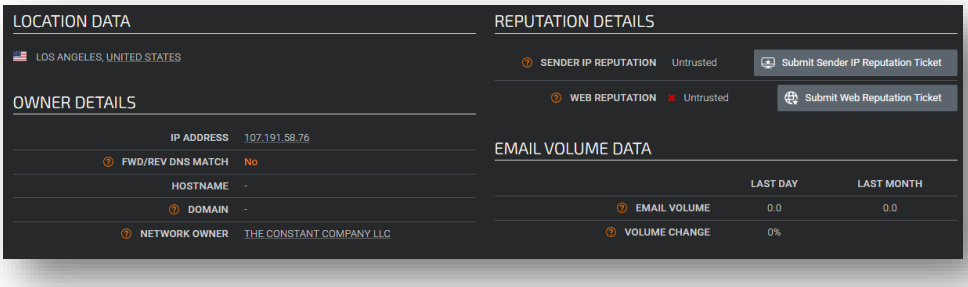
Source IP: 107.191.58.76

https://www.virustotal.com/gui/ip-address/107.191.58.76



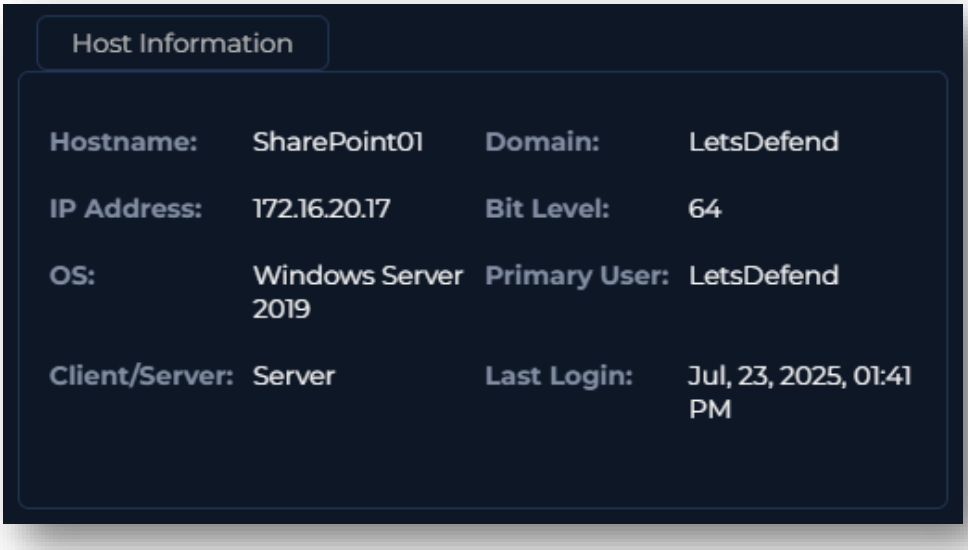
https://www.abuseipdb.com/check/107.191.58.76

https://talosintelligence.com/reputation_center/lookup?search=107.191.58.76



It is identified that the source address of this web attack traffic is malicious with an untrusted reputation; this alert should be treated as **suspicious**.

Destination IP: 172.16.20.17

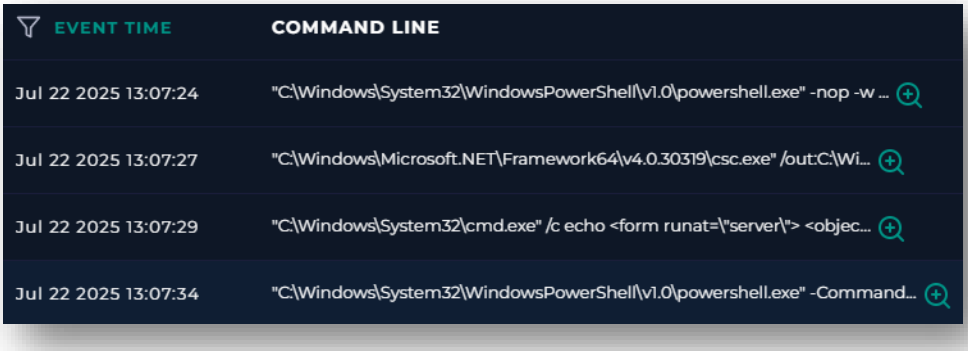


It is identified that the victim host machine of the web attack is a **Windows SharePoint Server**, vulnerable to the identified CVE exploit. All signs so far indicate suspicious activity.

Analysis

Now that we have detected the web attack, we can begin the analysis by investigating Endpoint Security.

We identified 4 events related to the alert in Terminal History.



EVENT TIME	COMMAND LINE
Jul 22 2025 13:07:24	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -nop -w ...
Jul 22 2025 13:07:27	"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /out:C:\Wi...
Jul 22 2025 13:07:29	"C:\Windows\System32\cmd.exe" /c echo <form runat=\"server\"> <objec...
Jul 22 2025 13:07:34	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -Command...

The first command uses **PowerShell** to create a **Base64 encoded** ASP.NET web shell-style diagnostic/**exfiltration script** whose purpose is to **extract** and disclose the application's **MachineKey configuration at runtime**.

The second command uses **csc.exe** (C# compiler) to compile the PowerShell script into the C# **payload.exe**.

The third command observes use of the IoC **spinstall0.aspx** to create a button on the **SignOut page** of the **SharePoint Server** that **redirects the user upon clicking** to URL http://107.191.58.76/payload.exe.

The fourth command sees the **attacker successfully retrieve the MachineKey** using [System.Web.Configuration.MachineKeySection]::GetApplicationConfig().

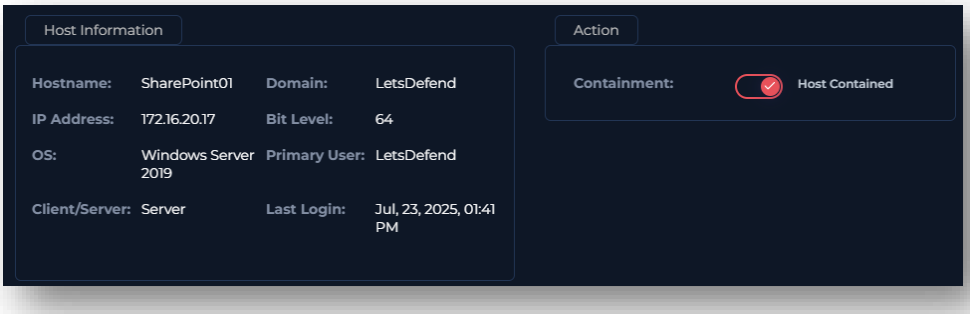
Now that we have identified that the activity on the Endpoint's Terminal is **malicious**, we need to further investigate the incident through Log Management.

We identified that 1 event (before Jul, 22, 2025, 01:07 PM UTC) was logged from source address **107.191.58.76** communicating with SharePoint01 destination address **172.16.20.17**.

The log was the alerted activity identified by the SIEM.

Containment

Based on the information gathered during the investigation, it is highly likely that the system has been compromised. Immediate isolation of the system from the network is required, and the alert is to be escalated to Tier 2.



Summary

The incident involves a compromised system named **SharePoint01** with an IP address of **172.16.20.17**. The alert was triggered by behaviour linked to **CVE-2025-53770**, which could allow an **unauthorized attacker** to **execute code over a network** in an on-premises **Microsoft SharePoint Server**, based on the rule SOC342 - CVE-2025-53770 SharePoint ToolShell Auth Bypass and RCE.

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.

After investigating Endpoint Security, it was identified that the attacker obfuscated an ASP.NET web shell-style **exfiltration script** with the purpose to **extract** the application's **MachineKey** configuration at runtime.

The attacker then used **csc.exe** to compile the script into the C# **payload.exe**. After this, we find evidence of the IoC **spinstall0.aspx**. It was found that the attacker created a button on the **SignOut page** of the **SharePoint Server** that redirects the user upon clicking to URL http://107.191.58.76/payload.exe, executing the malicious payload on the server.

This malicious payload sees the **attacker successfully retrieve the MachineKey** using [System.Web.Configuration.MachineKeySection]::GetApplicationConfig().

The MachineKey controls cryptographic operations in ASP.NET, including; encryption & validation, authentication ticket signing, anti-forgery tokens, role cookies, etc. If an attacker can read or manipulate these values, they can; forge authentication cookies, tamper with encryption & validation, and bypass integrity checks.

Based on the findings of the incident, immediate action needs to be taken to isolate the compromised system, and the event was identified as a **True Positive**.

Lessons Learned

- CVE-2025-53770 was an evolution of previously patched flaws (CVE-2025-49704 and CVE-2025-49706), demonstrating that incomplete initial mitigations can leave systems vulnerable to subsequent, more sophisticated attacks

- Attackers can achieve persistence by stealing cryptographic secrets, such as ASP.NET machine keys, this means simply applying a patch or removing a web shell is not enough; stolen keys allow attackers to forge authentication tokens and regain access indefinitely until the keys themselves are rotated

Remediation Actions

- Use or upgrade to supported versions of on-premises Microsoft SharePoint Server

- Apply the latest security updates

- Ensure the Antimalware Scan Interface is turned on and configured correctly and deploy Defender Antivirus on all SharePoint servers

- Rotate SharePoint Server ASP.NET machine keys

- Restart IIS on all SharePoint servers using iisreset.exe

Appendix

MITRE ATT&CK

MITRE Tactics	MITRE Techniques
Initial Access	T1190 - Exploit Public-Facing Application
Discovery	T1033 - System Owner/User Discovery
Execution	T1059.001 - Command and Scripting Interpreter: PowerShell
Execution	T1059.003 - Command and Scripting Interpreter: Windows Command Shell
Execution	T1543.003 - Create or Modify System Process: Windows Service
Persistence	T1505.003 - Server Software Component: Web Shell
Persistence	T1505.004 - Server Software Component: IIS Components
Defense Evasion	T1620 - Reflective Code Loading
Collection	T1119 - Automated Collection
Collection	T1005 - Data from Local System

Artifacts

Value	Comment	Type
/_layouts/15/ToolPane.aspx?DisplayMode=Edit&a=/ToolPane.aspx	Requested URL	URL Address
/_layouts/SignOut.aspx	Referer	URL Address
http://107.191.58.76/payload.exe	Malicious payload	URL Address
107.191.58.76	Attacker	IP Address
02b4571470d83163d103112f07f1c434	spinstall0.aspx	MD5 Hash

LetsDefend Playbook

LetsDefend Event ID: 320