NOTHREAT™

Detect. Protect. Neutralize.

# 40 Days Ahead of the Hack: SharePoint Attack Prevented with Nothreat

## A Nothreat Use Case with Azerconnect Group

Technology is trusted by FORTUNE 500 Companies & Public Sector

# The Most Recent Case in Detail: Tracking a Jun 2025 SharePoint 0-Day, Before the World Knew

**A 0-day is not simply "a bug."**

It is a time-sensitive imbalance between offense and defense. Whoever controls the knowledge of the flaw controls the battlefield

# The MS SharePoint CVE, first published on the 19th of July, 2025

## Customer guidance for SharePoint vulnerability CVE-2025-53770

MSRC / By MSRC / July 19, 2025 / 5 min read

| Revision | Change | Date |
|---|---|---|
| 1.0 | Information published | 07/19/25 |
| 2.0 | Clarified affected SharePoint product in summary | 07/20/25 |
| | Added fix availability guidance | |
| | Provided additional protections guidance regarding:<br>• Upgrade SharePoint products to supported versions (if required)<br>• Install July 2025 Security Updates<br>• Rotate machine keys | |

# The CVE has 9.8 out of 10 severity score

| 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 |

## Product Status

Learn more

| Vendor | Product | Platforms |
|---|---|---|
| Microsoft | Microsoft SharePoint Enterprise Server 2016 | x64-based Systems |

# Exploitation Chain

## Access Vectors:

- Unauthenticated access to vulnerable systems
- Authenticated access via network spoofing

## Impact:

- Full access to SharePoint content
- Exposure of file systems & internal configurations
- Remote code execution over the network

## Exploitation Techniques:

- Deployment of webshells (.aspx, .exe)
- Malicious .dll payloads observed

# Nothreat Detected and Prevented First Attacks in June, 2025


# How To Detect?

## CISA.GOV Published Ioc for Detection

**Specific IOCs:**

Malicious file hashes (e.g., **92bb4d..., .dll, .aspx** payloads)

IP addresses observed during exploitation (e.g., **107.191.58.76, 104.238.159.149**, etc.) ...

**Request Patterns & Payload Indicators:**

HTTP methods and targeted endpoints:

GET | POST on **/_layouts/15/ToolPane.aspx** with **DisplayMode=Edit**

Access to /_layouts/spinstall0.aspx, info3.aspx, SignOut.aspx, and similar patterns ...

# Attack Vectors We Collected

## ToolPane exploitation attempts

```
POST /_layouts/15/ToolPane.aspx?DisplayMode=Edit&a=/ToolPane.aspx

POST /_layouts/15/ToolPane.aspx/?DisplayMode=Edit&a=/ToolPane.aspx

POST /_layouts/15/ToolPane.aspx?DisplayMode=Edit

HEAD /_layouts/15/toolpane.aspx/lkx?DisplayMode=Edit&lkx=/ToolPane.aspx
```

# Attack Vectors We Collected

## Custom installation & info pages

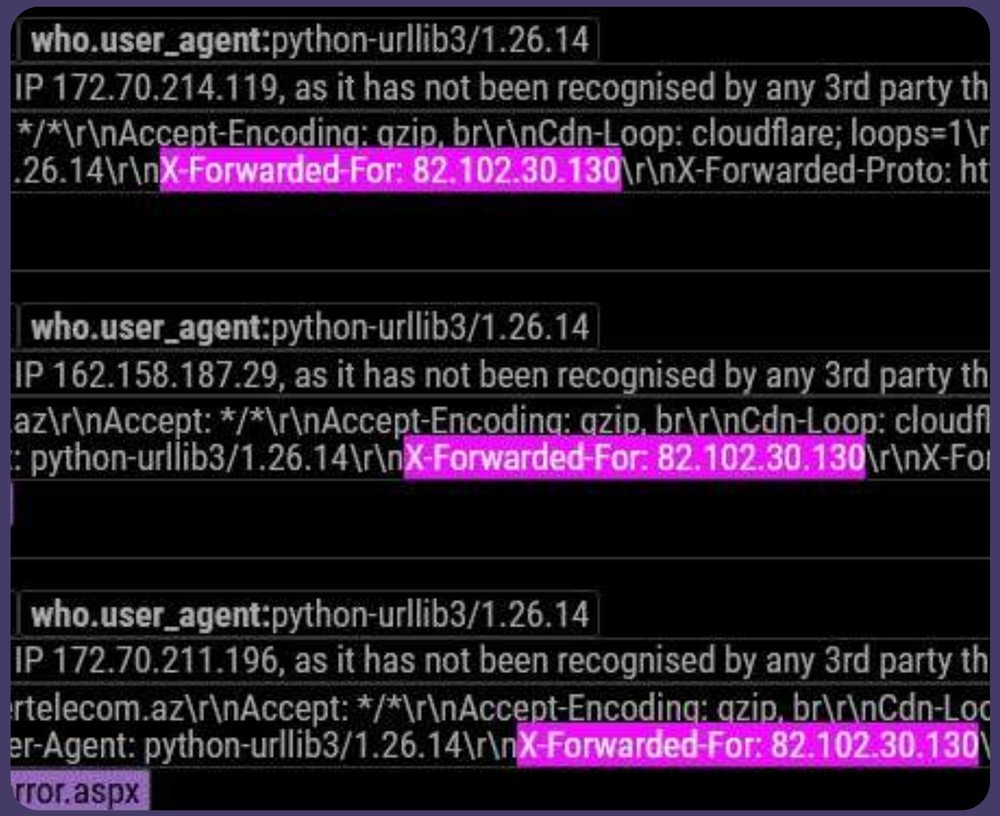
```
GET /_layouts/15/spinstall0.aspx
GET /_layouts/15/spinstall1.aspx
GET /_layouts/15/info03.aspx
GET /_layouts/15/info3.aspx
GET /_layouts/16/spinstall0.aspx
GET /_layouts/16/info3.aspx
GET /_layouts/15/pinstall.aspx
GET /_layouts/15/start.aspx
```

# Zero-Day Attacks Against Azerconnect Group

# First Attacks Detected and Prevented 40 Days Before the CVE was Published

Attack against Azerconnect Group: many different, regular IPs, but a single Attacker

# Attackers Love Free Hosting Too: Spotting Bad Guys Behind Cloud Giants, but Nothreat Detected Them




Akamai, Fastly, Cloud Flare,
AWS CloudFront, Azure
Front Door, Google Cloud CDN

**The pattern is always the same:**
Connecting IP = proxy/CDN
In Header = real client

# Nothreat Detects and Blocks Attackers Who Using Proxy

## 82.102.30.130, US

ISP: VENUS BUSINESS COMMUNICATIONS LIMITED
Usage Type: Data Center/Web Hosting/Transit
ASN: AS9009
Domain Namem247.com
Country: US, Los Angeles, California

Agent: **python-urllib3/1.26.14**

**Clear indicator of a scripted scanner/exploit kit**

Requests focused on SharePoint authentication & login flows:

Attacks appear in sequence, **within seconds** → a predefined wordlist probing SP auth & error handling.

Attempting to discover differences in HTTP status codes, redirects, or error pages.

Goal: identify whether the target is running vulnerable SharePoint and if auth redirection logic could be abused for a zero-day exploit chain (the June 2025 CVE).

# Distinguishing Real Attacker From Proxy

| | | |
|---|---|---|
| **AWS CloudFront** | `X-Forwarded-For` | No custom header, just standard XFF. |
| **AWS ALB / ELB** | `X-Forwarded-For` | |
| **Azure Front Door / CDN** | `X-Forwarded-For` | |
| **Google Cloud CDN / Armor** | `X-Forwarded-For` | |

| | | |
|---|---|---|
| **Cloudflare** | `CF-Connecting-IP`<br>`True-Client-IP` (enterprise option)<br>also sets `X-Forwarded-For` | Always trust only if the peer is in CF CIDRs. |
| **Akamai** | `True-Client-IP`<br>(sometimes also `X-Forwarded-For`) | `True-Client-IP` is their proprietary standard. |
| **Fastly** | `Fastly-Client-IP`<br>[illegible] | |

NOTHREAT™

Detect. Protect. Neutralize.

# Contact Us

## Upgrade to Proactive Cybersecurity

engage@nothreat.io

https://nothreat.io

307 Euston Road, London, UK, NW1 3AD

# Nothreat in the Media


Read Press Release

## Nothreat is the official Cybersecurity Partner of **Pafos FC**, Champions of Cyprus


Read Press Release

## Nothreat Strikes Partnership with Azerbaijani Number One Football Club **Qarabağ FK**

Latest clients and co-operations include

COP29 Baku Azerbaijan · azerconnect GROUP · Lenovo · PASHA Bank · pro><ima TECH SOLUTIONS · ISD DUBAI SPORTS CITY · F.C. ΠΑΦΟΣ · SAUGOS TARNYBA ARGUS