CISA Code & Media Analysis

############ README ###############
Edit rules and queries as needed for your hunt and based on your environment.
Ensure your EDR/SIEM instance has enough memory to run these AND/OR condition based queries. May take longer to run than conventional Sigma rule query.
Do not edit "logsource-product:" unless you are editing this rule to meet specific logsources/fields and know your environment.
TLP GREEN + Please use local installation of Sigma to convert this rule.
TLP CLEAR may convert rules using online converter of choice.
###################################

```
title: Detects CVE-2025-53770 CVE-2025-53771 Updated IOCs and Activity
incident: 251133.r2
tlp: CLEAR
id: 32bba1a1-3900-4cf9-b379-3e71a63998a3
status: test
description: Detects ToolShell CVE-2025-53770 Exploitation of SharePoint servers. Detects updated IOCs and Activity. CVE-2025-49704, CVE-2025-49706, CVE-2025-53770 and CVE-2025-53771. TA - Linen Typhoon, Violet Typhoon, Storm-2603.
references:
    - https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/?msockid=3e14885e8c2b643323129d998d366597
    - https://socradar.io/toolshell-sharepoint-zero-day-cve-2025-53770/
    - https://unit42.paloaltonetworks.com/microsoft-sharepoint-cve-2025-49704-cve-2025-49706-cve-2025-53770/
    - https://github.com/kaizensecurity/CVE-2025-53770/blob/master/payload
    - https://www.picussecurity.com/resource/blog/cve-2025-53770-critical-unauthenticated-rce-in-microsoft-sharepoint
    - https://www.trendmicro.com/en_us/research/25/g/cve-2025-53770-and-cve-2025-53771-sharepoint-attacks.html
author: CISA Code & Media Analysis
date: 2025-07-23
modified: 2025-07-23
tags:
    - cve.2025.49704
    - cve.2025.49706
    - cve.2025.53770
    - cve.2025.53771
logsource:
    product: cma
detection:
    keywords:
        - '92bb4ddb98eeaf11fc15bb32e71d0a63256a0ed826a03ba293ce3a8bf057a514'
        - '4a02a72aedc3356d8cb38f01f0e0b9f26ddc5ccb7c0f04a561337cf24aa84030'
```

```
        - 'b39c14becb62aeb55df7fd55c814afbb0d659687d947d917512fe67973100b70'
        - 'fa3a74a6c015c801f5341c02be2cbdfb301c6ed60633d49fc0bc723617741af7'
        - '390665bdd93a656f48c463bb6c11a4d45b7d5444bdd1d1f7a5879b0f6f9aac7e'
        - '66af332ce5f93ce21d2fe408dffd49d4ae31e364d6802fff97d95ed593ff3082'
        - '7baf220eb89f2a216fcb2d0e9aa021b2a10324f0641caf8b7a9088e4e45bec95'
        - '8d3d3f3a17d233bc8562765e61f7314ca7a08130ac0fb153ffd091612920b0f2'
        - '30955794792a7ce045660bb1e1917eef36f1d5865891b8110bf982382b305b27'
        - 'b336f936be13b3d01a8544ea3906193608022b40c28dd8f1f281e361c9b64e93'

        - '107.191.58.76'
        - '104.238.159.149'
        - '96.9.125.147'
        - '103.186.30.186'
        - '45.77.155.170'
        - '139.144.199.41'
        - '172.174.82.132'
        - '89.46.223.88'
        - '45.77.155.170'
        - '154.223.19.106'
        - '185.197.248.131'
        - '149.40.50.15'
        - '64.176.50.109'
        - '149.28.124.70'
        - '206.166.251.228'
        - '95.179.158.42'
        - '86.48.9.38'
        - '128.199.240.182'
        - '212.125.27.102'
        - '91.132.95.60'
        - '134.199.202.205'
        - '131.226.2.6'
        - '188.130.206.168'

        - 'Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101
Firefox/120.0'
        -
'Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:120.0)+Gecko/20100101+Firefox/120.0'
        - 'c34718cbb4c6.ngrok-free.app/file.ps1'

    keywords_1:
        - '*\TEMPLATE\LAYOUTS\*'
    keywords_2:
        - 'spinstall*'
        - 'debug*'
        - 'info*'
    keywords_3:
        - '*.aspx'
        - '*.js'

    keywords_4:
```

```
    - 'POST'
    - 'GET'
    - 'curl'
keywords_5:
    - '*/_layouts/*'
    - '*/layouts/*'
    - '*layouts*'
keywords_6:
    - '*ToolPane.aspx'
    - '*DisplayMode'
    - '*SignOut.aspx'
    - '*spinstall*'
    - 'VIEWSTATE'

keywords_7:
    - 'cmd.exe'
keywords_8:
    - 'powershell.exe'
keywords_9:
    - '-EncodedCommand'
    - '-ec'
    - '-enc'
    - 'VIEWSTATE'
    - 'yoserial*'

keywords_10:
    - '*\TEMPLATE\LAYOUTS\*'
keywords_11:
    - 'ChildItem'
keywords_12:
    - 'targetFile'
keywords_13:
    - 'NewLine'
keywords_14:
    - '*web.config*'

keywords_15:
    - 'Ry2cuVmFsaWRhd'
    - 'Validation'
keywords_16:
    - 'ifCIRy2cuQ29tc'
    - 'Decryption'
keywords_17:
    - 'dGlvb'
    - 'Key'
keywords_18:
    - 'UZtleVNlY3Rpb2'
    - 'MachineKey'
keywords_19:
    - 'ShudWxsLC'
```

```
        - 'Invoke'
    keywords_20:
        - 'XIiIGxhbmd1Y'
        - 'language'
    keywords_21:
        - 'qZWN0WzBdKTsNC'
        - 'new object'

    keywords_22:
        - 'POST'
        - 'powershell*'
        - '*layouts*'
    keywords_23:
        - 'ToolPane.aspx'
        - '*spinstall*'


    condition: keywords or keywords_1 and keywords_2 and keywords_3 or keywords_4
and keywords_5 and keywords_6 or keywords_7 and keywords_8 and keywords_9 or
keywords_10 and keywords_11 and keywords_12 and keywords_13 and keywords_14 or
keywords_15 and keywords_16 and keywords_17 and keywords_18 and keywords_19 and
keywords_20 and keywords_21 or keywords_22 and keywords_23

falsepositives:
    - Rate of FP low-moderate with some strings.
    - Use this rule in an infected environment/logs.
    - Analyst may need to make adjustments to the query as required.
level: critical
```