Security Advisory 2025-027

Critical Vulnerabilities in Microsoft SharePoint

2025-07-24 — v1.3

TLP:CLEAR

History:

- *21/07/2025 — v1.0 – Initial publication*
- *21/07/2025 — v1.1 – Updated information*
- *22/07/2025 — v1.2 – Updated information from Microsoft*
- *24/07/2025 — v1.3 – Further updated information from Microsoft*

Summary

On July 19, 2025, Microsoft released an out-of-bound advisory addressing two vulnerabilities on Microsoft SharePoint, one of which being rated as critical and allowing unauthenticated remote attacker to execute arbitrary code on vulnerable systems [1,2]. These vulnerabilities apply to on-premises SharePoint Servers only. SharePoint Online in Microsoft 365 is not impacted. **These critical flaws are actively being exploited in the wild since at least 18th of July 2025** [4].

It is recommended isolating vulnerable system from the Internet, but also from internal systems, and running a compromise assessment before updating.

Technical Details

The vulnerability **CVE-2025-53770**, with a CVSS score of 9.8, is due to the deserialisation of untrusted data. This flaw allows an unauthorised attacker to execute code over a network [2].

The vulnerability **CVE-2025-53771**, with a CVSS score of 6.3, is a spoofing vulnerability due to improper limitation of a path name to a restricted directory (*path traversal*) [3].

Affected Products

The vulnerabilities **CVE-2025-53770** and **CVE-2025-53771** affect:

- Microsoft SharePoint Server Subscription Edition
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Enterprise Server 2016

  [Updated] *Note: All prior versions of SharePoint are no longer supported and should be considered vulnerable, but **will not be patched** by Microsoft.*

Recommendations

It is recommended isolating vulnerable system from the Internet, but also from internal systems, and running a compromise assessment before updating.

[Updated] After running a compromise assessment and updating affected servers, it is strongly recommended rotating SharePoint Server ASP.NET machine keys, before restarting the IIS service using `iisreset.exe` [1,5].

Mitigation

The vendor strongly advises deploying Microsoft Defender for Endpoint protection, or equivalent threat solutions, as well as enabling and properly configuring the Antimalware Scan Interface [1].

Threat Hunting

To identify possible exploitation of the vulnerabilities, it is possible to execute the following queries in the Microsoft 365 security centre's Advanced Hunting page [1,6].

Advanced Hunting in Microsoft Defender XDR

> *NOTE: The following sample queries search for a week's worth of events. For longer timespans, the default settings of Advanced Hunting would need to be adapted [1].*

Successful exploitation using file creation

Search for the creation of `spinstall0.aspx`, which indicates successful post-exploitation of CVE-2025-53770:

```
DeviceFileEvents
| where FolderPath has_any ("microsoft shared\\Web Server Extensions\\15\\TEMPLATE\\LAYOUTS",
  "microsoft shared\\Web Server Extensions\\16\\TEMPLATE\\LAYOUTS")
| where FileName contains "spinstall"
| project Timestamp, DeviceName, InitiatingProcessFileName, InitiatingProcessCommandLine,
  FileName, FolderPath, ReportId, ActionType, SHA256
| order by Timestamp desc
```

Post-exploitation PowerShell dropping web shell

Search for process creations, where `w3wp.exe` is spawning encoded PowerShell involving the `spinstall0` file or the file paths it has been known to be written to:

```
DeviceProcessEvents
| where InitiatingProcessFileName has "w3wp.exe"
    and InitiatingProcessCommandLine !has "DefaultAppPool"
    and FileName =~ "cmd.exe"
    and ProcessCommandLine has_all ("cmd.exe", "powershell")
    and ProcessCommandLine has_any ("EncodedCommand", "-ec")
| extend CommandArguments = split(ProcessCommandLine, " ")
| mv-expand CommandArguments to typeof(string)
| where CommandArguments matches regex "^[A-Za-z0-9+/=]{15,}$"
| extend B64Decode = replace("\\x00", "", base64_decodestring(tostring(CommandArguments)))
| where B64Decode contains "spinstall",
  @'C:\PROGRA~1\COMMON~1\MICROS~1\WEBSER~1\15\TEMPLATE\LAYOUTS',
```

```
  @'C:\PROGRA~1\COMMON~1\MICROS~1\WEBSER~1\16\TEMPLATE\LAYOUTS')
```

Post-exploitation web shell dropped

Search for the web shell dropped using the PowerShell command:

```
DeviceFileEvents
| where Timestamp >ago(7d)
| where InitiatingProcessFileName=~"powershell.exe"
| where FileName contains "spinstall"
```

Exploitation detected by Defender

Search at Microsoft Defender for Endpoint telemetry to determine if specific alerts fired in your environment:

```
AlertEvidence
| where Timestamp > ago(7d)
| where Title has "SuspSignoutReq"
| extend _DeviceKey = iff(isnotempty(DeviceId), bag_pack_columns(DeviceId, DeviceName),"")
| summarize min(Timestamp), max(Timestamp), count_distinctif(DeviceId,isnotempty(DeviceId)),
  make_set(Title), make_set_if(_DeviceKey, isnotempty(_DeviceKey) )
```

Unified Advanced Hunting query

Find exposed devices

Search for devices vulnerable to the CVEs listed in blog [5]:

```
DeviceTvmSoftwareVulnerabilities
| where CveId in ("CVE-2025-49706","CVE-2025-53770")
```

Web shell C2 communication

Find devices that may have communicated with Storm-2603 web shell C2, that may indicate a compromised device beaconing to Storm-2603 controlled infrastructure:

```
let domainList = "update.updatemicfosoft.com";
union
(
    DnsEvents
    | where QueryType has_any(domainList) or Name has_any(domainList) or QueryType matches
  regex @"^.*\.devtunnels\.ms$" or Name matches regex @"^.*\.devtunnels\.ms$"
    | project TimeGenerated, Domain = QueryType, SourceTable = "DnsEvents"
),
(
    IdentityQueryEvents
    | where QueryTarget has_any(domainList) or QueryType matches regex @"^.*\.devtunnels\.ms$"
    | project Timestamp, Domain = QueryTarget, SourceTable = "IdentityQueryEvents"
),
(
    DeviceNetworkEvents
    | where RemoteUrl has_any(domainList) or RemoteUrl matches regex @"^.*\.devtunnels\.ms$"
    | project Timestamp, Domain = RemoteUrl, SourceTable = "DeviceNetworkEvents"
```

```
),
(
    DeviceNetworkInfo
    | extend DnsAddresses = parse_json(DnsAddresses), ConnectedNetworks =
  parse_json(ConnectedNetworks)
    | mv-expand DnsAddresses, ConnectedNetworks
    | where DnsAddresses has_any(domainList) or ConnectedNetworks.Name has_any(domainList) or
  DnsAddresses matches regex @"^.*\.devtunnels\.ms$" or ConnectedNetworks .Name matches regex
  @"^.*\.devtunnels\.ms$"
    | project Timestamp, Domain = coalesce(DnsAddresses, ConnectedNetworks.Name), SourceTable =
   "DeviceNetworkInfo"
),
(
    VMConnection
    | extend RemoteDnsQuestions = parse_json(RemoteDnsQuestions), RemoteDnsCanonicalNames =
  parse_json(RemoteDnsCanonicalNames)
    | mv-expand RemoteDnsQuestions, RemoteDnsCanonicalNames
    | where RemoteDnsQuestions has_any(domainList) or RemoteDnsCanonicalNames
  has_any(domainList) or RemoteDnsQuestions matches regex @"^.*\.devtunnels\.ms$" or
  RemoteDnsCanonicalNames matches regex @"^.*\.devtunnels\.ms$"
    | project TimeGenerated, Domain = coalesce(RemoteDnsQuestions, RemoteDnsCanonicalNames),
  SourceTable = "VMConnection"
),
(
    W3CIISLog
    | where csHost has_any(domainList) or csReferer has_any(domainList) or csHost matches regex
   @"^.*\.devtunnels\.ms$" or csReferer matches regex @"^.*\.devtunnels\.ms$"
    | project TimeGenerated, Domain = coalesce(csHost, csReferer), SourceTable = "W3CIISLog"
),
(
    EmailUrlInfo
    | where UrlDomain has_any(domainList) or UrlDomain matches regex @"^.*\.devtunnels\.ms$"
    | project Timestamp, Domain = UrlDomain, SourceTable = "EmailUrlInfo"
),
(
    UrlClickEvents
    | where Url has_any(domainList) or Url matches regex @"^.*\.devtunnels\.ms$"
    | project Timestamp, Domain = Url, SourceTable = "UrlClickEvents"
)
| order by TimeGenerated desc
```

Hunting in Microsoft Sentinel

Detect network indicators of compromise and file hashes using ASIM

```
//IP list and domain list- _Im_NetworkSession
let lookback = 30d;
let ioc_ip_addr = dynamic(["131.226.2.6", "134.199.202.205", "104.238.159.149",
  "188.130.206.168"]);
let ioc_domains = dynamic(["c34718cbb4c6.ngrok-free.app"]);
_Im_NetworkSession(starttime=todatetime(ago(lookback)), endtime=now())
| where DstIpAddr in (ioc_ip_addr) or DstDomain has_any (ioc_domains)
| summarize imNWS_mintime=min(TimeGenerated), imNWS_maxtime=max(TimeGenerated),
  EventCount=count() by SrcIpAddr, DstIpAddr, DstDomain, Dvc, EventProduct, EventVendor
```

```
//IP list - _Im_WebSession
let lookback = 30d;
let ioc_ip_addr = dynamic(["131.226.2.6", "134.199.202.205", "104.238.159.149",
```

```
  "188.130.206.168"]);
let ioc_sha_hashes
  =dynamic(["92bb4ddb98eeaf11fc15bb32e71d0a63256a0ed826a03ba293ce3a8bf057a514"]);
_Im_WebSession(starttime=todatetime(ago(lookback)), endtime=now())
| where DstIpAddr in (ioc_ip_addr) or FileSHA256 in (ioc_sha_hashes)
| summarize imWS_mintime=min(TimeGenerated), imWS_maxtime=max(TimeGenerated),
  EventCount=count() by SrcIpAddr, DstIpAddr, Url, Dvc, EventProduct, EventVendor
```

```
// file hash list - imFileEvent
let ioc_sha_hashes =
  dynamic(["92bb4ddb98eeaf11fc15bb32e71d0a63256a0ed826a03ba293ce3a8bf057a514"]);
imFileEvent
| where SrcFileSHA256 in (ioc_sha_hashes) or TargetFileSHA256 in (ioc_sha_hashes)
| extend AccountName = tostring(split(User, @'')[1]),
  AccountNTDomain = tostring(split(User, @'')[0])
| extend AlgorithmType = "SHA256"
```

Post exploitation C2 or file hashes

Find devices that may have communicated with Storm-2603 post exploitation C2 or contain known Storm-2603 file hashes:

```
//IP list - _Im_WebSession
let lookback = 30d;
let ioc_ip_addr = dynamic(["65.38.121.198"]);
let ioc_sha_hashes
  =dynamic(["92bb4ddb98eeaf11fc15bb32e71d0a63256a0ed826a03ba293ce3a8bf057a514",
"24480dbe306597da1ba393b6e30d542673066f98826cc07ac4b9033137f37dbf",
"b5a78616f709859a0d9f830d28ff2f9dbbb2387df1753739407917e96dadf6b0",
"c27b725ff66fdfb11dd6487a3815d1d1eba89d61b0e919e4d06ed3ac6a74fe94",
"1eb914c09c873f0a7bcf81475ab0f6bdfaccc6b63bf7e5f2dbf19295106af192",
"4c1750a14915bf2c0b093c2cb59063912dfa039a2adfe6d26d6914804e2ae928",
"83705c75731e1d590b08f9357bc3b0f04741e92a033618736387512b40dab060",
"f54ae00a9bae73da001c4d3d690d26ddf5e8e006b5562f936df472ec5e299441",
"b180ab0a5845ed619939154f67526d2b04d28713fcc1904fbd666275538f431d",
"6753b840cec65dfba0d7d326ec768bff2495784c60db6a139f51c5e83349ac4d",
"7ae971e40528d364fa52f3bb5e0660ac25ef63e082e3bbd54f153e27b31eae68",
"567cb8e8c8bd0d909870c656b292b57bcb24eb55a8582b884e0a228e298e7443",
"445a37279d3a229ed18513e85f0c8d861c6f560e0f914a5869df14a74b679b86",
"ffbc9dfc284b147e07a430fe9471e66c716a84a1f18976474a54bee82605fa9a",
"6b273c2179518dacb1218201fd37ee2492a5e1713be907e69bf7ea56ceca53a5",
"c2c1fec7856e8d49f5d49267e69993837575dbbec99cd702c5be134a85b2c139"]);
_Im_WebSession(starttime=todatetime(ago(lookback)), endtime=now())
| where DstIpAddr in (ioc_ip_addr) or FileSHA256 in (ioc_sha_hashes)
| summarize imWS_mintime=min(TimeGenerated), imWS_maxtime=max(TimeGenerated),
  EventCount=count() by SrcIpAddr, DstIpAddr, Url, Dvc, EventProduct, EventVendor
```

Storm-2603 C2 communication

Search for devices that may have communicated with Storm-2603 C2 infrastructure as part of this activity:

```
//IP list and domain list- _Im_NetworkSession
let lookback = 30d;
let ioc_ip_addr = dynamic(["65.38.121.198"]);
let ioc_domains = dynamic(["update.updatemicfosoft.com"]);
```

```
_Im_NetworkSession(starttime=todatetime(ago(lookback)), endtime=now())
| where DstIpAddr in (ioc_ip_addr) or DstDomain has_any (ioc_domains)
| summarize imNWS_mintime=min(TimeGenerated), imNWS_maxtime=max(TimeGenerated),
  EventCount=count() by SrcIpAddr, DstIpAddr, DstDomain, Dvc, EventProduct, EventVendor
```

References

[1] https://msrc.microsoft.com/blog/2025/07/customer-guidance-for-sharepoint-vulnerability-cve-2025-53770/

[2] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53770

[3] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53771

[4] https://research.eye.security/sharepoint-under-siege/

[5] https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/#mitigation-and-protection-guidance

[6] https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/#indicators-of-compromise