مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Zero-Day Exploitation of SharePoint Server

Tracking #:432317507

Date:20-07-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Microsoft has issued an urgent advisory addressing a critical remote code execution (RCE) vulnerability, CVE-2025-53770, actively exploited in the wild.

TECHNICAL DETAILS:

Microsoft has issued an urgent advisory addressing a critical remote code execution (RCE) vulnerability, CVE-2025-53770, actively exploited in the wild. This flaw stems from the deserialization of untrusted data in on-premises SharePoint Server, enabling unauthenticated attackers to remotely execute arbitrary code and gain full administrative control.

The vulnerability is a **variant of CVE-2025-49706** and is currently **unpatched**. As exploitation is ongoing, customers using vulnerable on-premises SharePoint Server instances are at **immediate risk** of full system compromise. Microsoft is working to release a security update and has issued **mitigation guidance** and **detection recommendations**.

Vulnerability Details:

- CVE ID: CVE-2025-53770
- Type: Remote Code Execution via Deserialization
- CVSS Score: 9.8 (Critical)
- Attack Vector: Network (Unauthenticated)
- Impacted Systems: On-premises SharePoint Server only, SharePoint Online in Microsoft 365 is not impacted.
- Exploit Status: Actively exploited in the wild
- Patch Status: No patch available as of July 20, 2025

Threat Capabilities

- Exploitation allows:
  - Remote arbitrary code execution
  - Complete administrator access
  - Installation of web shells
  - Persistent control of compromised servers

Detection Guidance
Microsoft Defender Antivirus Detections:

- Exploit:Script/SuspSignoutReq.A
- Trojan:Win32/HijackSharePointServer.A

Microsoft Defender for Endpoint Alerts:

- Possible web shell installation
- Possible exploitation of SharePoint server vulnerabilities
- Suspicious IIS worker process behavior
- 'SuspSignoutReq' malware blocked
- 'HijackSharePointServer' malware blocked

Advanced Hunting Query (Microsoft 365 Defender)

- Look for **creation of spinstall0.aspx**, which signals **successful post-exploitation**
- (SHA-256: 92bb4ddb98eeaf11fc15bb32e71d0a63256a0ed826a03ba293ce3a8bf057a514)

Mitigation Steps (Immediate Action Required):

1. **Enable AMSI Integration (Antimalware Scan Interface)**:
2. **Install Microsoft Defender Antivirus** on **all SharePoint servers** to block threat components:
    - Ensure real-time protection is enabled.
3. **If AMSI Cannot Be Enabled**:
    - **Disconnect SharePoint Server from the Internet** to prevent unauthenticated access.
4. Monitor for IOC (spinstall0.aspx, Defender alerts)
5. Implement network monitoring for outbound connections from SharePoint servers
6. Block external access to SharePoint servers at firewall level until patched
7. Enable comprehensive logging for all SharePoint activities and process execution
8. Isolate affected systems immediately and preserve forensic evidence
9. Rotate all credentials with SharePoint access, prioritizing service accounts

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to follow Microsoft's recommended mitigation steps to secure environment until an official security update is released.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://msrc.microsoft.com/blog/2025/07/customer-guidance-for-sharepoint-vulnerability-cve-2025-53770/
- https://nvd.nist.gov/vuln/detail/CVE-2025-53770