

What is ToolShell?

ToolShell is the name for a remote code execution chain in on-premises Microsoft SharePoint Server, tracked as CVE-2025-53770 (deserialization of untrusted data, CVSS 9.8) and CVE-2025-53771 (an authentication bypass through path traversal). They are bypasses of CVE-2025-49704 and CVE-2025-49706, first shown at Pwn2Own in May 2025 and patched in July. Attackers posted to ToolPane.aspx without logging in, dropped a web shell and stole the ASP.NET machine keys. SharePoint 2016, 2019 and Subscription Edition were affected; SharePoint Online was not.

HOW IT WORKS

01 How the attack worked

Shown for defensive context, the campaign followed a consistent pattern:

- A crafted POST to `/_layouts/15/ToolPane.aspx?DisplayMode=Edit` with `Referer: /_layouts/SignOut.aspx`, carrying the deserialization payload.
- A [web shell](/learn/persistence/what-is-a-web-shell) written as `spinstall0.aspx` (and variants) in the `_layouts/15/` folder.
- Machine key theft. The shell read the ASP.NET `ValidationKey` and `DecryptionKey` from `web.config`. With those keys an attacker can sign their own `__VIEWSTATE` payloads, which SharePoint then deserializes as trusted, so they keep code execution even after the bug is patched.
- Follow-on activity: credential theft with `Mimikatz`, lateral movement with `PsExec` and `Impacket`, disabling Microsoft Defender and, in some intrusions, ransomware.

Espionage and ransomware groups both used the chain against finance, education, energy, healthcare and government targets.

PATCHING ALONE DID NOT EVICT ATTACKERS

Stolen machine keys stay valid after the patch. Any server that was exposed before the fix needs its ASP.NET machine keys rotated, or the attacker can keep forging `ViewState` payloads.

HOW TO DEFEND

- Install the July 2025 SharePoint security updates or later for SharePoint Server 2016, 2019 and Subscription Edition. Out-of-support versions such as SharePoint 2013 get no fix.
- Rotate the ASP.NET machine keys after patching, with `Update-SPMachineKey` in PowerShell or the Machine Key Rotation timer job, then restart IIS on every server in the farm.
- Turn on AMSI integration (the Antimalware Scan Interface, Full Mode) with an endpoint protection product, which Microsoft recommended as a compensating control.
- Hunt for `spinstall0.aspx` or other unexpected `.aspx` files in `_layouts`, POSTs to `ToolPane.aspx` with a sign-out referer in IIS logs, and `w3wp.exe` spawning `cmd.exe` or `powershell.exe`.
- Reduce exposure. Do not publish on-premises SharePoint directly to the internet without an authenticating gateway in front of it.

SOURCES

- [1] NVD: CVE-2025-53770
- [2] NVD: CVE-2025-53771
- [3] MITRE ATT&CK: SharePoint ToolShell Exploitation (C0058)
- [4] MITRE CWE-502: Deserialization of Untrusted Data

Find the path to a shell before an attacker does.

`securelayer7.net/learn/web-exploitation/what-is-toolshell`

[Open online](#)