



|630 Freedom Business Center Drive, Suite 212|
|King of Prussia, PA 19406|
|610.768.1100|

Microsoft SharePoint Server Compromise

July 25 2025

On July 19, 2025, Microsoft Security Response Center (MSRC) published a blog addressing active attacks against on-premises SharePoint servers that exploit

- CVE-2025-49706, a spoofing vulnerability, and
- CVE-2025-49704, a remote code execution vulnerability.

These vulnerabilities only affect on-premises SharePoint servers and do not affect SharePoint Online in Microsoft 365 cloud.

Microsoft has released new comprehensive security updates for all supported versions of SharePoint Server (Subscription Edition, 2019, and 2016) that protect customers against these new vulnerabilities.

TS Partners is Unaffected and No Action is Required

- The flaw is present in older on-premises versions of SharePoint.
- It does not impact the newer, cloud-based version of SharePoint that Microsoft has been encouraging customers to adopt.
- TS Partners does not self-host and uses SharePoint Online in Microsoft 365 Cloud.

Steps for Affected On-Premises Users

United States Cybersecurity and Infrastructure Security Agency (CISA) said in guidance that:

- “CISA recommends disconnecting public-facing versions of SharePoint Server that have reached their end-of-life (EOL) or end-of-service (EOS)
- For example, SharePoint Server 2013 and earlier versions are end-of-life and should be discontinued if still in use.”
- Users should apply all updates, enable malware scanning, rotate machine keys, isolate vulnerable servers, reset credentials, scan for indicators of compromise, and check backups and logs.

Additional Information:

<https://www.cisa.gov/news-events/alerts/2025/07/20/update-microsoft-releases-guidance-exploitation-sharepoint-vulnerabilities>

<https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/?is=18c94605e858e45703b160acfc6ec7406bfece0a08088a24496b88ca1f1a2168#storm-2603>

For questions regarding Policy, contact CEO or COO

Last Review: July 25 2025 **Last Revision:** July 25 2025