



Bulletin d'alerte

Vulnérabilité exploitée dans Microsoft SharePoint

SOMMAIRE

Contexte	2
CVE-2025-53770	2
Type de vulnérabilité	2
Risque.....	2
Criticité (score de base CVSS v3.1)	2
Produits impactés	2
Recommandations	3
Preuve de concept.....	3
Indicateurs de compromission	4
Références	5

CONTEXTE

Le 18 juillet 2025, les chercheurs en sécurité de l'entreprise néerlandaise [Eye Security](#) identifient l'exploitation de la [CVE-2025-53770](#) (*zero day*) ciblant des serveurs Sharepoint. Jointe à la [CVE-2025-53771](#), ces vulnérabilités forment deux variantes de la chaîne d'attaque baptisée [ToolShell](#) et composée des [CVE-2025-49706](#) et [CVE-2025-49704](#) corrigées en juillet 2025. Une **preuve de concept** avait été publiée trois jours plus tôt concernant ces deux dernières, par des chercheurs de la société [Code White GmbH](#).



A date, seule la [CVE-2025-53770](#) est confirmée **exploitée** par Microsoft, et plus de 9300 serveurs dans le monde seraient vulnérables. Des indicateurs de compromission sont disponibles.

CVE-2025-53770



Une désérialisation non sécurisée des données dans les serveurs Microsoft SharePoint permet à un attaquant non authentifié, en envoyant des requêtes spécifiquement forgées, de déposer des portes dérobées sur le serveur afin d'exécuter du code arbitraire.

Type de vulnérabilité

[CWE-502](#): Deserialization of Untrusted Data

Risque

→ Exécution de code arbitraire

Criticité (score de base CVSS v3.1)

Vecteur d'attaque	Réseau	Portée	Inchangée
Complexité d'attaque	Faible	Impact sur la confidentialité	Élevé
Privilèges requis	Aucun	Impact sur l'intégrité	Élevé
Interaction de l'utilisateur	Aucune	Impact sur la disponibilité	Élevé

Produits impactés

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

Recommandations

Mettre à jour Microsoft SharePoint Server Subscription Edition vers la version *build* 16.0.18526.20508.

Mettre à jour Microsoft SharePoint Server 2019 vers la version *build* 16.0.10417.20037.

En attendant un correctif pour SharePoint Server 2016, l'éditeur recommande également de :

- Activer l'intégration de l' *Antimalware Scan Interface* (AMSI) en mode complet,
- Déployer Defender Antivirus sur les serveurs,
- S'il n'est pas possible d'appliquer les correctifs, déconnecter les serveurs SharePoint vulnérables du réseau.

Des informations complémentaires sont disponibles dans le [bulletin](#) de Microsoft.

Preuve de concept

Actuellement, aucune preuve de concept n'est disponible en sources ouvertes.

INDICATEURS DE COMPROMISSION

TLP	TYPE	VALEUR	OBSERVATION
TLP:CLEAR	Adresse IP	107.191.58[.]76	Première vague d'exploitation IP source basée aux États-Unis responsable de l'exploitation active le 18 juillet vers 18h06 UTC déployant spinstall0.aspx
TLP:CLEAR	Adresse IP	104.238.159[.]149	Deuxième vague d'exploitation IP source basée aux États-Unis responsable de l'exploitation active le 19 juillet vers 07h28 UTC
TLP:CLEAR	Adresse IP	96.9.125[.]147	Partagé par PaloAlto Unit42
TLP:CLEAR	Adresse IP	103.186.30[.]186	Partagé par @andrewdanis sur X
TLP:CLEAR	Requête POST	/_layouts/15/ToolPane.aspx?DisplayMode=Edit&a=/ToolPane.aspx	Requête POST utilisée pour déclencher l'exploit et pousser Sharpyshell lié à CVE-2025-49706 et/ou CVE-2025-53770
TLP:CLEAR	En-tête	/_layouts/SignOut.aspx	En-tête HTTP exact utilisé dans l'exploitation de ToolPane.aspx dans la requête POST liée à CVE-2025-53770
TLP:CLEAR	SHA256	92bb4ddb98eeaf11fc15bb32e71d0a63256a0ed826a03ba293ce3a8bf057a514	Hash de spinstall0.aspx probablement créé avec Sharpyshell
TLP:CLEAR	MD5	02b4571470d83163d103112f07f1c434	Hash de spinstall0.aspx probablement créé avec Sharpyshell
TLP:CLEAR	SHA-1	f5b60a8ead96703080e73a1f79c3e70ff44df271	Hash de spinstall0.aspx probablement créé avec Sharpyshell
TLP:CLEAR	SHA256	4a02a72aedc3356d8cb38f01f0e0b9f26ddc5ccb7c0f04a561337cf24aa84030	Hash partagé par PaloAlto Unit42
TLP:CLEAR	SHA256	b39c14becb62aeb55df7fd55c814afbb0d659687d947d917512fe67973100b70	Hash partagé par PaloAlto Unit42
TLP:CLEAR	SHA256	fa3a74a6c015c801f5341c02be2cbdfb301c6ed60633d49fc0bc723617741af7	Hash partagé par PaloAlto Unit42
TLP:CLEAR	Fichier	spinstall0.aspx	Fichier aspx malveillant

RÉFÉRENCES

- <https://www.cve.org/CVERecord?id=CVE-2025-53770>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53770/>
- <https://msrc.microsoft.com/blog/2025/07/customer-guidance-for-sharepoint-vulnerability-cve-2025-53770/>
- <https://www.cve.org/CVERecord?id=CVE-2025-53771>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53771/>
- <https://research.eye.security/sharepoint-under-siege/>
- <https://thehackernews.com/2025/07/critical-microsoft-sharepoint-flaw.html>
- <https://x.com/Shadowserver/status/1946900837306868163>