DJ-CERT | Centre national de veille, d'alerte et de réponse aux attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 27-07-2025

BULLETIN ALERTES

Object	Multiples vulnérabilités dans Microsoft SharePoint
Réference	1367
Date de Publication	2025-07-24
Sévérité	Critique

IMPACT :

- Exécution de code arbitraire à distance
- Contournement de la politique de sécurité

SYSTÉME AFFECTÉ :

- Microsoft SharePoint Server 2019 sans le correctif KB5002754
- Microsoft SharePoint Subscription Edition sans le correctif KB5002768
- Microsoft SharePoint Enterprise Server 2016 sans le correctif KB5002760
- Microsoft SharePoint Enterprise Server 2016 Language Pack sans le correctif KB5002759
- Microsoft confirme que les versions 2010 et 2013 de SharePoint Enterprise Server ne recevront pas de mise à jour de sécurité. Il est fortement recommandé de migrer vers une version à jour.

DÉSCRIPTION :

Les 21 et 22 juillet 2025, Microsoft a publié plusieurs mises à jour de sécurité critiques pour SharePoint Enterprise Server 2016, en réponse à la découverte de deux vulnérabilités zero-day activement exploitées (CVE-2025-53770 et CVE-2025-53771). Ces failles permettent le contournement des correctifs précédemment appliqués et sont utilisées dans le cadre d'attaques ciblées, identifiées sous le nom de **"ToolShell"**, contre les serveurs SharePoint. Leur exploitation peut permettre l'exécution de code arbitraire à distance ainsi que le contournement des politiques de sécurité. Des marqueurs de compromission (IOCs) ont également été publiés pour faciliter la détection d'une activité malveillante.

SOLUTION :

- Appliquer les dernières mises à jour de sécurité.
- Procéder à une rotation des clés de machine ASP.NET sur les serveurs SharePoint.
- Redémarrer IIS sur l'ensemble des serveurs SharePoint.
- Isoler d'Internet les versions obsolètes de SharePoint (notamment SharePoint 2013 et antérieures) arrivées en fin de vie (EOL/EOS).
- Mettre à jour les règles de l'IPS (Intrusion Prevention System) et du WAF (Web Application Firewall) afin de bloquer les modèles d'exploitation connus et les comportements suspects.
- Réduire les privilèges sur les pages de mise en page (layouts) ainsi que les accès administratifs.
- Surveiller toute activité liée aux indicateurs de compromission (IOCs), en particulier à partir du 7 juillet 2025.
- Alerter le DJCERT en cas de détection d'une activité relative à une exploitation de ces vulnérabilités.

DOCUMENTATION :

- Bulletin de sécurité Microsoft du 20 Juillet 2025:

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

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

- Prévention de l'exploitation active des vulnérabilités SharePoint guide :

https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/

- CVE-2025-53770:

https://nvd.nist.gov/vuln/detail/CVE-2025-53770

- CVE-2025-53771:

https://nvd.nist.gov/vuln/detail/CVE-2025-53771