ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

BULLETIN DE SÉCURITÉ

Titre	[Mise à jour 24/07/ 2025] Vulnérabilités critiques dans Microsoft SharePoint
Numéro de Référence	56002407/25
Date de Publication	24 Juillet 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- 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,

[Mise à jour du 24 juillet 2025]

- 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.

Identificateurs externes

- CVE-2025-53770, CVE-2025-53771,

Bilan de la vulnérabilité

[Mise à jour du 22 juillet 2025]

Microsoft a publié les mises à jour de sécurité pour SharePoint Enterprise Server 2016, ainsi, des marqueurs de compromission à rechercher.

[Mise à jour du 21 juillet 2025]

Microsoft a publié des mises à jour de sécurité d'urgence pour deux nouvelles vulnérabilités critiques « zero-day » dans SharePoint, identifiées par « CVE-2025-53770 et CVE-2025-53771 ». Ces failles permettent aux attaquants de contourner les correctifs précédents et sont activement exploitées dans des attaques "ToolShell" ciblant les serveurs SharePoint.

L'exploitation de ces vulnérabilités peut permettre à un attaquant d'exécuter du code arbitraire à distance et de contourner la politique de sécurité.

Solution :

Le maCERT recommande les actions suivantes :

- Appliquer les dernières mises à jour de sécurité
- Effectuer une rotation des clés de machine ASP.NET du SharePoint Server
- Redémarrer IIS sur tous les serveurs SharePoint
- Déconnecter d'Internet les versions obsolètes de SharePoint (ex. SharePoint 2013 et antérieurs) qui ont atteint leur fin de vie (EOL/EOS).
- Mettre à jour les règles IPS (Intrusion Prevention System) et WAF (Web Application Firewall) pour bloquer les modèles d'exploit connus et les comportements anormaux.
- Limiter les privilèges sur les pages de mise en page (layouts) et les accès administrateurs.
- Scanner toute activité liée aux IOCs (particulièrement depuis le 07 juillet 2025).
- Alerter le maCERT en cas de détection d'une activité relative à une exploitation de ces vulnérabilités.

Risque :

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

Indicateurs de compromission (IOCs):

Hashs :

- 92bb4ddb98eeaf11fc15bb32e71d0a63256a0ed826a03ba293ce3a8bf057a514
- 24480dbe306597da1ba393b6e30d542673066f98826cc07ac4b9033137f37dbf
- b5a78616f709859a0d9f830d28ff2f9dbbb2387df1753739407917e96dadf6b0
- c27b725ff66fdfb11dd6487a3815d1d1eba89d61b0e919e4d06ed3ac6a74fe94
- 1eb914c09c873f0a7bcf81475ab0f6bdfaccc6b63bf7e5f2dbf19295106af192
- 4c1750a14915bf2c0b093c2cb59063912dfa039a2adfe6d26d6914804e2ae928
- 83705c75731e1d590b08f9357bc3b0f04741e92a033618736387512b40dab060
- f54ae00a9bae73da001c4d3d690d26ddf5e8e006b5562f936df472ec5e299441
- b180ab0a5845ed619939154f67526d2b04d28713fcc1904fbd666275538f431d
- 6753b840cec65dfba0d7d326ec768bff2495784c60db6a139f51c5e83349ac4d
- 7ae971e40528d364fa52f3bb5e0660ac25ef63e082e3bbd54f153e27b31eae68

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

- 567cb8e8c8bd0d909870c656b292b57bcb24eb55a8582b884e0a228e298e7443
- 445a37279d3a229ed18513e85f0c8d861c6f560e0f914a5869df14a74b679b86
- ffbc9dfc284b147e07a430fe9471e66c716a84a1f18976474a54bee82605fa9a
- 6b273c2179518dacb1218201fd37ee2492a5e1713be907e69bf7ea56ceca53a5
- c2c1fec7856e8d49f5d49267e69993837575dbbec99cd702c5be134a85b2c139
- 6f6db63ece791c6dc1054f1e1231b5bbcf6c051a49bad0784569271753e24619
- d6da885c90a5d1fb88d0a3f0b5d9817a82d5772d5510a0773c80ca581ce2486d
- 62881359e75c9e8899c4bc9f452ef9743e68ce467f8b3e4398bebacde9550dea

Ip :

- 131.226.2.6
- 134.199.202.205
- 104.238.159.149
- 188.130.206.168
- 65.38.121.198
- 107.191.58.76
- 96.9.125.147

Domains :

- c34718cbb4c6.ngrok-free.app
- msupdate.updatemicfosoft.com

File Name / File Path:

- Spinstall0.aspx
- IIS_Server_dll.dll
- SharpHostInfo.x64.exe
- xd.exe
- debug_dev.js
- \1[5-6]\TEMPLATE\LAYOUTS\debug_dev.js

Annexe

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/

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma