Centre de Veille de Détection et
de Réaction aux Attaques
Informatiques

مركز اليقظة والرصد
والتصدي للهجمات المعلوماتية

Bulletin de sécurité du maCERT

Titre: Vulnérabilité de type Zero-day dans Microsoft Exchange (Suite)

Numéro de Référence : 19420602/19

Risque : Critique
Impact : Critique

Systèmes affectés

- Microsoft Exchange Server 2010 Service Pack 3 Update Rollup 26
- Microsoft Exchange Server 2013 Cumulative Update 22
- Microsoft Exchange Server 2016 Cumulative Update 12
- Microsoft Exchange Server 2019 Cumulative Update 1

Bilan de la vulnérabilité

Microsoft a publié une mise à jour pour limiter l'exploitation d'une faille critique au niveau du Serveur Microsoft Exchange. L'exploitation de cette faille peut permette à un utilisateur malveillant disposant d'un compte exchange de réussir une élévation de privilèges et obtenir le droit Admin sur le Contrôleur de Domaine.

Pour remédier à cette vulnérabilité, une politique de limitation pour **EWSMaxSubscriptions** peut être définie et appliquée avec la valeur zéro. Cela empêchera le serveur Exchange d'envoyer des notifications EWS et empêchera les applications clientes qui reposent sur les notifications EWS de fonctionner normalement.

Solution

- Veuillez-vous référer au bulletin de sécurité Microsoft du 05 Février 2019 :
- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV190007
- https://www.dgssi.gov.ma/fr/content/1935280119-vulnerabilite-de-type-zero-day-dans-microsoft-exchange.html

Risque :

- Elévation de privilèges ;
- Perte de contrôle du système affecté.

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: 05 37 57 21 47 – فاكس: 05 37 57 20 53
البريد الإلكتروني contact@macert.gov.ma

Annexe

- Bulletin de sécurité Microsoft du 05 Février 2019 :
- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV190007
- Bulletin de sécurité maCERT du 28 Janvier 2019 :
- https://www.dgssi.gov.ma/fr/content/1935280119-vulnerabilite-de-type-zero-day-dans-microsoft-exchange.html

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