17 mar 2021 -13:29

400 systèmes informatique belges infiltrés dans le cadre d'une vulnérabilité des serveurs Microsoft Exchange

Les conséquences de la vulnérabilité de Microsoft Exchange server pour les organisations et entreprises belges sont de plus en plus évidentes. La semaine dernière, nous avons déjà mis en garde contre cette vulnérabilité. À partir des listes de serveurs vulnérables, nous avons pu détecter plus de 400 systèmes où une forme d'intrusion s'est produite. Cela signifie que des parties malveillantes ont pénétré dans ces systèmes et attendent maintenant de passer à l'action. Nous craignons que des organisations et des entreprises soient victimes de ransomware ou que des données soient volées dans les jours et les semaines à venir.

Beaucoup de serveurs vulnérables ont été mis à jour, mais plus de 1000 systèmes sont encore vulnérables. Les entreprises et les organisations qui ont effectué les mises à jour doivent toutefois rester vigilantes et continuer à surveiller leurs systèmes. En effet, des traces peuvent encore être laissées entre l'intrusion et les mises à jour.

Le Centre pour la Cybersecurité Belgique est en train de contacter les organisations et entreprises infectées ou victimes d’une intrusion dont les coordonnées sont disponibles.

Qu'y a-t-il à craindre ?

Les cybercriminels installent ce qu'on appelle des *web shells*, qui leur donnent un accès et un contrôle à distance via un serveur en ligne. Cela leur permet de garder une ligne de communication ouverte, pour ainsi dire, afin de lancer une attaque ultérieurement. Dans les listes que nous avons examinées, nous avons trouvé au moins 400 serveurs avec un *web shell* installé. Dans d'autres cas, les pirates peuvent avoir installé d'autres logiciels malveillants, en plus des *web shells* en question, afin de monter une attaque à une date ultérieure, par exemple un ransomware.

Que doivent faire les entreprises et les organisations?

CERT.be, le service opérationnel du CCB a publié des avis (mis à jour le 16/3).

Les entreprises et les organisations qui utilisent Exchange Online avec une configuration hybride ou un serveur Exchange sur site pour les applications administratives doivent immédiatement prendre les mesures suivantes:

- Mettre à jour les systèmes.
- Retirer les *web shells*.
- Vérifier ce qui est arrivé avec le *web shell*.
- Détecter toute activité suspecte.

Cependant, le service Microsoft Exchange online n'est pas affecté.

Il est conseillé aux entreprises et aux organisations qui rencontrent des difficultés avec ces étapes de faire

appel à un partenaire TIC ou à un expert externe pour effectuer ces actions.

Plus d'information :

- Le conseil complet du CERT.be (mis à jour le 16/3)
- Communiqué de presse CCB (mis à jour le 16/3)
- Les utilisateurs moins expérimentés peuvent utiliser ce manuel de Microsoft. One-Click Microsoft Exchange On-Premises Mitigation Tool
- Extensive Incident Response guide (Updated by Microsoft on 16 March 2021)

Centre pour la Cybersécurité Belgique
Rue de la Loi 16
1000 Bruxelles
Belgique
http://www.ccb.belgium.be

Andries Bomans
Responsable communication
+32 471 66 00 06
andries.bomans@ccb.belgium.be

Katrien - Eggers
Responsable communication
+32 485 76 53 36
katrien.eggers@cert.be