SECURITY MADEIN.LU

circl.lu cases.lu c3.lu

INFO

[18.03.2021]

Exploitation des vulnérabilités dans Microsoft Exchange

Plusieurs vulnérabilités jugées critiques ont été découvertes dans les serveurs Microsoft Exchange 2010, 2013, 2016 et 2019 non corrigés (les serveurs Exchange Online ne sont pas concernés). L'exploitation de ces failles de sécurité entraîne un risque de vol ou de destruction des données et de compromission des infrastructures pour les entreprises impactées.

Ces vulnérabilités étaient jusqu'alors exploitées par un groupe d'activités – nommé HAFNIUM par Microsoft, depuis fin 2020. Une fois l'annonce de l'existence de ces vulnérabilités rendue publique début mars, l'exploitation de ces dernières s'est intensifiée, notamment pour le déploiement du nouveau ransomware *« DearCry »* et de malwares de minage de cryptomonnaie.

Une situation alarmante en raison du nombre de serveurs potentiellement concernés dans le monde. Au Luxembourg, un nombre significatif de serveurs Microsoft Exchange est jugé vulnérable.

CIRCL (Computer Incident Response Center Luxembourg), l'équipe de réponse sur incident « cyber » pour le secteur privé, les communes et entités non-gouvernementales au Luxembourg, a pour objectif de venir en aide aux entités composantes de l'économie luxembourgeoise lorsque la sécurité de leurs systèmes informatiques est mise en danger.

Les experts du CIRCL peuvent venir en aide individuellement à toutes les entreprises et organisations potentiellement affectées afin de les accompagner dans le processus de détection et de résolution des éventuelles intrusions.
Un Rapport Technique (TR-61) incluant toutes les recommandations pour la fixation et l'atténuation des bugs et risques potentiels a été élaboré. Dans celui-ci, il est recommandé, à ce jour, de considérer tout serveur Microsoft Exchange non corrigé comme compromis et de suivre la procédure suivante (cf. page suivante) :

- Prioriser l'installation des mises à jour sur les serveurs Microsoft Exchange, déployées par Microsoft. Tous les serveurs Microsoft Exchange impactés doivent impérativement être mis à jour.
- CIRCL averti cependant qu'appliquer les correctifs ne suffit pas. Ces correctifs ne sécuriseront pas les serveurs déjà compromis, puisque certains d'entre eux s'avéraient déjà exploités avant la disponibilité des correctifs. Les criminels pourraient donc avoir déjà installé des portes d'entrées dérobées. Il est nécessaire de scanner les serveurs Microsoft Exchange potentiellement compromis à l'aide des scripts suivants :
    - https://github.com/microsoft/CSS-Exchange/tree/main/Security
    - https://github.com/cert-lv/exchange_webshell_detection
- Enfin, il est vivement recommandé de revoir la sécurité et les « logs » des serveurs Microsoft Exchange afin de détecteur tout indicateur d'exploitation et d'appliquer les procédures standards de réponse à un incident. CIRCL peut vous accompagner si besoin.

Les indicateurs de compromissions (IoC) spécifiques sont également disponibles dans de nombreuses communautés de partage MISP (MISP event uuid: fd875781-262e-4159-a0cd-ac0241784cc7). Demande d'accès ici.

Des risques d'exploitation qui peuvent être accentués par les vulnérabilités dans le serveur Microsoft DNS :

Le 10 mars 2021, CERT-EU a publié un avis de sécurité (2021-014) faisant part de 5 vulnérabilités (dont l'une d'elles est jugée critique par Microsoft, CVE-2021-26897) dans les serveurs Windows 2016, 2019, 2012 (R2 inclus), 2008 (R2, R2 SP1 et R2 SP2 inclus), version 2004, version 1909 and version 20H2. Pour être exploitable, le serveur doit avoir le rôle DNS activé et la mise à jour dynamique activée (configuration par défaut).

Bien qu'aucune preuve d'exploitation en cours de ces vulnérabilités ne soit encore publique, il est recommandé d'appliquer les correctifs dès que possible et de donner la priorité aux mises à jour des serveurs DNS Windows Internet.
Deux mesures d'atténuation peuvent être prises afin de limiter l'exploitabilité des vulnérabilités :

- désactiver la fonction Dynamic Update
- activer les mises à jour de zones sécurisées

Cependant, l'activation des mises à jour de zones sécurisées protège contre les attaques sur les interfaces publiques, mais pas contre un criminel ayant déjà un pied dans le réseau (ordinateur lié à un domaine), ce qui vient augmenter les risques induits par les vulnérabilités dans certains serveurs Microsoft Exchange.

Pour toute question en lien avec cette situation, n'hésitez pas à prendre contact avec :

- Votre département IT, pour s'assurer que toutes les mises à jour et analyses nécessaires ont été effectuées
- Votre intégrateur IT
- Votre support Microsoft ou consultez le manuel de Microsoft : One-Click Microsoft Exchange On-Premises Mitigation Tool
- CIRCL :

circl.lu
Computer Incident Response Center
LUXEMBOURG

- **Par téléphone** : (+352) 247 88444
- **Par e-mail** : info@circl.lu

A propos de SECURITYMADEIN.LU

SECURITYMADEIN.LU est l'agence de cybersécurité au service de l'économie luxembourgeoise et des communes.
L'agence contribue et soutient le maintien de la fiabilité de l'économie luxembourgeoise en guidant ses acteurs vers des activités cyber-responsables, ceci via ses 3 départements : CIRCL (Computer Incident Response Center Luxembourg), CASES (Cyberworld Awareness Security Enhancement Services – Luxembourg) et C3 (Cybersecurity Competence Center – Luxembourg).
www.securitymadein.lu
www.cases.lu
www.circl.lu
www.c3.lu

Publié par SECURITYMADEIN.LU