Multiples vulnérabilités critiques dans Microsoft Exchange

Les Technologies de l'information souhaitent vous informer que Microsoft a publié des mises à jour *hors cycle* dans le but de corriger quatre vulnérabilités affectant son produit Exchange.

Ces vulnérabilités font actuellement l'objet d'une exploitation active par un réseau de cybercriminels connu sous le nom de HAFNIUM. Selon le chercheur de la firme *Volexity* (opérant dans le domaine de la cybersécurité), les attaques sont ciblées et sont perpétrées depuis le 6 janvier 2021.

Vulnérabilités

- CVE-2021-26855 : Il s'agit d'une vulnérabilité de falsification de requêtes côté serveur (SSRF) dans Exchange qui permet à l'acteur d'envoyer des requêtes HTTP arbitraires et de s'authentifier en tant que serveur Exchange.
- CVE-2021-26857 : L'exploitation de cette vulnérabilité donne aux acteurs la possibilité d'exécuter du code en tant que l'utilisateur SYSTEM sur le serveur Exchange. Cette vulnérabilité fait partie d'une chaîne d'attaque; son exploitation nécessite une autorisation d'administrateur (ou la présence d'une autre vulnérabilité).
- CVE-2021-26858 et CVE-2021-27065 : Ce sont des vulnérabilités d'écriture de fichier arbitraire post-authentification dans Exchange. Un acteur authentifié pourrait utiliser ces vulnérabilités pour écrire un fichier dans un emplacement arbitraire sur le serveur.

Versions affectées

Microsoft Exchange version 2019 et antérieures.

Recommandations

Les unités disposant du produit Exchange, version 2019 et antérieures, doivent appliquer les mises à jour proposées par Microsoft.

Pour toutes questions d'ordre technique, veuillez communiquer avec l'équipe *Sécurité* des Technologies de l'information, par courriel, à l'adresse « securite @umontreal.ca ».

Nous vous remercions de votre collaboration.