MICROSOFT EXCHANGE : Des attaques 0-Day ont déjà touché 30.000 serveurs dans le monde

Les autorités mettent en garde contre "l'exploitation nationale et internationale généralisée des vulnérabilités de Microsoft Exchange Server", alors il est impératif de mettre à jour ce logiciel dès maintenant.

Les recherches effectuées par les experts en sécurité dans le monde ont permis de découvrir que 4 vulnérabilités jusque-là inconnues ou «zero-day» dans Microsoft Exchange Server sont désormais utilisées dans des attaques généralisées contre des milliers d'organisations.

Microsoft a attribué les attaques à une équipe de piratage nouvellement découverte qu'elle appelle Hafnium, un groupe vraisemblablement soutenu par la Chine. Microsoft a déclaré qu'il s'agissait «d'attaques ciblées limitées», mais a averti qu'elles pourraient être plus largement exploitées dans un proche avenir.

Les bogues sont suivis en tant que CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 et CVE-2021-27065. Le CI-CERT encourage vivement tous les clients Exchange Server à appliquer immédiatement les mises à jour.

De ce que nous savons aujourd'hui, Hafnium cible principalement les entités américaines dans la recherche sur les maladies infectieuses, les cabinets d'avocats, les établissements d'enseignement supérieur, les entrepreneurs de la défense, les groupes de réflexion politiques et les ONG, selon Microsoft.

Le résumé des vulnérabilités :

- CVE-2021-26855 :est une vulnérabilité de falsification de requête côté serveur (SSRF) dans Exchange qui permettait à l'attaquant d'envoyer des requêtes HTTP arbitraires et de s'authentifier en tant que serveur Exchange.

- CVE-2021-26857 : est une vulnérabilité de désérialisation non sécurisée dans le service de messagerie unifiée. La désérialisation non sécurisée est l'endroit où des données contrôlables par l'utilisateur non approuvées sont désérialisées par un programme. L'exploitation de cette vulnérabilité a donné à Hafnium la possibilité d'exécuter du code en tant que SYSTEM sur le serveur Exchange. Cela nécessite une autorisation d'administrateur ou une autre vulnérabilité à exploiter.

- CVE-2021-26858 : est une vulnérabilité d'écriture de fichier arbitraire post-authentification dans Exchange. Si Hafnium pouvait s'authentifier auprès du serveur Exchange, alors ils pourraient utiliser cette vulnérabilité pour écrire un fichier sur n'importe quel chemin sur le serveur. Ils pourraient s'authentifier en exploitant la vulnérabilité SSRF CVE-2021-26855 ou en compromettant les informations d'identification d'un administrateur légitime.

- CVE-2021-27065 : est une vulnérabilité d'écriture de fichier arbitraire post-authentification dans Exchange. Si Hafnium pouvait s'authentifier auprès du serveur Exchange, alors ils pourraient utiliser cette vulnérabilité pour écrire un fichier sur n'importe quel chemin sur le serveur. Ils pourraient s'authentifier en exploitant la vulnérabilité SSRF CVE-2021-26855 ou en compromettant les informations d'identification d'un administrateur légitime.

NB : Selon certaines sources, les attaques auraient débuté depuis le début de l'année (Janvier 2021).

Vous pouvez vérifier à l'aide de l'outil Test-ProxyLogon.ps1 si vous êtes vulnérables aux 0 Days de Microsoft Exchange Server.