Configurer le déchiffrement sur un serveur MS Exchange

Publié: 2024-11-03

Le déchiffrement TLS est un outil puissant pour améliorer la visibilité de votre réseau. La vulnérabilité de MS Exchange, CVE-2021-26855, constitue une raison impérieuse de configurer le déchiffrement sur les serveurs Exchange. Cette vulnérabilité permet aux attaquants de mener des attaques par falsification de requêtes côté serveur (SSRF) en envoyant des requêtes HTTP personnalisées via des connexions non authentifiées. Ces demandes sont généralement cryptées via HTTPS. La seule façon de savoir si une demande contient ces instructions personnalisées est de déchiffrer les charges utiles HTTPS.

Par installation d'un redirecteur de clé de session sur votre serveur Exchange, vous pouvez vous assurer qu'ExtraHop peut déchiffrer le trafic Exchange en toute sécurité. Le CVE-2021-26855 ayant été exploité via HTTPS, nous vous recommandons de déchiffrer spécifiquement le trafic HTTP en suivant les instructions de la section suivante : Ajouter un port global au mappage de protocoles.

En savoir plus sur Décryptage TLS.