De graves failles dans les NAS Synology à corriger | Le Net Expert Informatique

De graves failles dans les NAS Synology à corriger

Le fabricant de NAS Synology a corrigé plusieurs vulnérabilités dans son OS maison DSM (DiskStation Manager) – et ses composants associés – qui anime ses appliances de stockage, dont l'une pouvait permettre à des attaquants de compromettre les données stockées.

En effet, la vulnérabilité la plus sérieuse concerne donc Synology Photo Station, une fonction du DSM, le système d'exploitation basé sur Linux. Photo Station permet aux utilisateurs de créer des albums photo en ligne et des blogs accessibles à distance via l'adresse IP publique du périphérique. Mais des chercheurs en sécurité de l'entreprise néerlandaise Securify ont découvert que Photo Station n'effaçait pas correctement les entrées utilisateur, laissant à des attaquants la possibilité d'injecter des commandes système qui pourraient être exécutées avec les privilèges du serveur web.
De plus, Photo Station n'est pas protégé contre le cross-site request forgery (CSRF), une technique qui permet à un site web de forcer le navigateur d'un visiteur à exécuter des actions malveillantes sur un site différent de celui sur lequel il se connecte. Donc, même si Photo Station n'est pas configuré pour être accessible depuis Internet, un attaquant pourrait inciter un utilisateur situé sur le même réseau que le périphérique NAS à visiter une page web malveillante qui utiliserait le CSRF pour exploiter la vulnérabilité par commande d'injection sur le réseau LAN local. « En tirant parti de cette faille, des attaquants pourraient compromettre le périphérique NAS, et toutes les données qui y sont stockées », ont expliqué les chercheurs dans un avis qui comprend également une preuve de concept de l'exploit.

Des ransomwares s'attaquent à Synology
La version 6.3-2945 de Photo Station livrée la semaine dernière par Synology corrige cette vulnérabilité. Mais les notes de version font simplement état « d'améliorations de sécurité » sans donner de détails. La nouvelle version corrige aussi deux vulnérabilités cross-site scripting (XSS) identifiées par les chercheurs de Securify. Celles-ci pourraient être exploitées pour tromper les utilisateurs de Photo Station en les incitant à cliquer sur une URL malveillante qui exécute un code voyou dans leurs navigateurs. En cas de succès de ces attaques, des pirates pourraient voler les jetons de session ou les identifiants de connexion des utilisateurs de Photo Station ou exécuter des actions arbitraires en usurpant leur identité.
La semaine dernière Synology a corrigé une vulnérabilité similaire dans l'interface de gestion de DiskStation Manager. Les utilisateurs sont invités à mettre DSM à jour en version 5.2-5565 Update 1. Dans le passé, les boitiers NAS de Synology ont déjà été la cible de pirates. Ainsi, pas plus tard que l'an dernier, des attaquants ont exploité une vulnérabilité pour infecter plusieurs boitiers avec un ransomware destiné à crypter les fichiers stockés. Auparavant, les pirates avaient réussi à s'introduire dans les boitiers NAS de Synology pour faire tourner des programmes qui généraient de la crypto-monnaie pour leur compte.

Source : http://www.lemondeinformatique.fr/actualites/lire-synology-corrige-de-graves-failles-dans-son-os-dsm-61277.html
Par Jean Elyan