mFIN-CERT.tg

Systèmes obsolètes et réglages d'usine: des failles héritées

Par Kossi DOH
Lead RedTeam departement CDA

Le deuxième groupe de failles ne provient pas d'une erreur de configuration ponctuelle, mais d'un manque d'entretien dans la durée: des logiciels qu'on ne met plus à jour, et des équipements qu'on installe sans changer leurs réglages d'origine.

Des logiciels et systèmes qui ne sont plus entretenus

Tout logiciel, aussi bien conçu soit-il, finit par révéler des failles avec le temps. C'est pour cela que les éditeurs publient des mises à jour de sécurité. Un système obsolète est un système qui a cessé de recevoir ces correctifs, ou dont les correctifs disponibles n'ont pas été installés. Nos tests ont identifié plusieurs systèmes et modules dans cette situation, avec des failles connues permettant une exécution de code à distance: en clair, un attaquant peut faire exécuter à la machine des instructions de son choix, sans avoir besoin d'un mot de passe ni d'un accès physique. C'est la catégorie de faille la plus critique, car elle peut donner à un attaquant un contrôle quasi total de la machine touchée.

Des mots de passe d'usine jamais changés

De nombreux équipements réseau (routeurs, pare-feux, caméras, imprimantes, onduleurs connectés…) sont livrés avec un compte administrateur et un mot de passe par défaut, identiques pour tous les appareils du même modèle et souvent publiés dans la documentation du fabricant. Lorsque ce mot de passe n'est jamais modifié à l'installation, n'importe qui connaissant la marque et le modèle de l'équipement, une information parfois visible sur une simple etiquette, peut s'y connecter et en modifier la configuration. Nos missions ont retrouvé cette situation sur plusieurs équipements, ce qui revient à installer une porte blindée tout en laissant la clé du fabricant sous le paillasson.

Ce qu'il faut retenir: Un équipement ou un logiciel qu'on installe puis qu'on oublie devient, avec le temps, l'une des portes d'entrée les plus faciles à exploiter.

Recommandations

- Maintenir un inventaire des systèmes et logiciels, avec un calendrier régulier de mises à jour de sécurité.
- Retirer ou isoler les systèmes qui ne sont plus supportés par leur éditeur, lorsqu'ils ne peuvent pas être remplacés immédiatement.
- Changer systématiquement les identifiants par défaut de tout nouvel équipement avant sa mise en service.
- Restreindre l'accès aux interfaces d'administration des équipements au strict personnel autorisé.