mFIN-CERT.tg

Cybersécurité dans les institutions de microfinance au Togo. Ce que révèlent nos tests d'intrusion.

Par Kossi DOH
Lead RedTeam departement CDA

Ce volet de notre série de sensibilisation présente trois nouvelles familles de vulnérabilités identifiées par Cyber Defense Africa (CDA) lors de ses missions de test d'intrusion auprès d'institutions de microfinance au Togo. L'objectif est d'expliquer ces risques en langage clair, sans viser une institution en particulier, afin de renforcer la vigilance collective du secteur. Les cas présentés ici ont un point commun: ils reposent sur des failles bien documentées, parfois connues depuis plusieurs années, pour lesquelles des correctifs existent. Leur exploitation réussie rappelle qu'une vulnérabilité publiée n'est dangereuse que tant qu'elle n'est pas corrigée et qu'elle le reste, activement, jusqu'à ce qu'elle le soit.

Article 1: Des failles connues, mais jamais corrigées

La majorité des grandes cyberattaques ne reposent pas sur des techniques secrètes ou sophistiquées, mais sur l'exploitation de failles déjà connues et documentées publiquement, pour lesquelles un correctif existe... mais n'a pas été appliqué. Nos tests d'intrusion en ont retrouvé deux illustrations marquantes.

La faille Cisco qui crée des comptes administrateur (CVE-2023-20198)
Cette vulnérabilité touche l'interface d'administration web de certains équipements réseau Cisco (routeurs, commutateurs). Elle permet à un attaquant, sans identifiant ni mot de passe, de créer lui-même un compte disposant des droits les plus élevés sur l'équipement. Une fois ce compte créé, l'attaquant contrôle l'appareil comme s'il en était l'administrateur légitime: il peut consulter et modifier la configuration du réseau, intercepter du trafic, ou s'en servir comme point d'entrée vers le reste du système d'information. C'est comme si un visiteur pouvait, depuis l'accueil d'un bâtiment, se délivrer lui-même un badge "directeur" sans que personne ne le remarque.

EternalBlue: une faille de 2017 encore active en 2024
EternalBlue est le nom donné à une vulnérabilité du protocole de partage de fichiers Windows (SMB), rendue tristement célèbre en 2017 par les cyberattaques mondiales WannaCry et NotPetya, qui avaient paralysé hôpitaux, usines et administrations dans le monde entier. Un correctif existe depuis cette date. Nos tests ont pourtant permis d'exploiter cette même faille sur plusieurs postes et serveurs, ce qui a donné un accès complet à ces machines et permis de récupérer les identifiants de nombreux utilisateurs jusqu'à ceux donnant accès à la base de données centrale de l'institution. Une seule machine non corrigée a ainsi suffi à mettre en péril l'ensemble du système d'information.

Ce qu'il faut retenir
Une faille publiée et corrigible depuis des années reste une porte grande ouverte tant que le correctif n'a pas été réellement appliqué sur chaque machine concernée.

Recommandations

- Mettre à jour sans délai le système d'exploitation des équipements Cisco concernés et désactiver l'interface d'administration web lorsqu'elle n'est pas indispensable.
- Déployer un processus systématique et régulier d'application des correctifs de sécurité (patch management) sur l'ensemble du parc, serveurs comme postes de travail.
- Retirer définitivement le protocole SMBv1, vecteur d'EternalBlue, de tous les systèmes.
- Mettre en place un inventaire des équipements et un suivi des vulnérabilités connues qui les concernent.