mFIN-CERT.tg

Applications métier, la vigilance jusqu'au dernier maillon

Par Kossi DOH
Lead RedTeam departement CDA

Le troisième groupe de failles concerne les applications utilisées au quotidien par les agents des institutions: logiciels de gestion des comptes clients, des crédits, ou outils internes. Une application peut être installée sur un réseau parfaitement protégé et rester malgré tout vulnérable si elle n'a pas été conçue ou configurée avec la sécurité en tête.

Des applications que n'importe qui peut utiliser

Nos tests ont identifié des applications accessibles sur le réseau sans qu'aucune authentification ne soit demandée : pas de nom d'utilisateur, pas de mot de passe. Toute personne ayant simplement accès au réseau peut alors consulter, et parfois modifier, les données ou fonctions de l'application, exactement comme un bureau dont la porte resterait ouverte en permanence, sans réception ni contrôle d'accès.

Des journaux consultables sans se connecter

Les logs, ou journaux d'activité, enregistrent les actions effectuées sur une application: connexions, opérations, erreurs. Ils sont précieux pour détecter un incident, mais ils contiennent aussi des informations sensibles. Une mauvaise gestion des droits d'accès a permis, dans certains cas, de consulter ces journaux sans être connecté à l'application, exposant ainsi des informations qui auraient dû rester internes.

La traversée de répertoire: sortir du dossier prévu

Certaines applications qui permettent de consulter ou télécharger un fichier ne vérifient pas suffisamment le nom du fichier demandé. Un attaquant peut alors manipuler ce nom pour remonter dans l'arborescence du serveur et accéder à des fichiers qui ne devaient pas être exposés, parfois des fichiers de configuration contenant eux-mêmes des mots de passe. C'est comme demander un document précis à un guichet, mais découvrir qu'en modifiant légèrement sa demande, on peut se faire remettre n'importe quel dossier de l'armoire, y compris ceux qui ne concernent pas le demandeur.

Ce qu'il faut retenir

La sécurité d'une institution ne se limite pas à son réseau: chaque application doit, elle aussi, vérifier qui a le droit d'y accéder et à quoi.

Recommandations

- Exiger une authentification sur toute application accédant à des données ou fonctions sensibles, sans exception.
- Restreindre l'accès aux journaux applicatifs aux seuls comptes autorisés et les auditer régulièrement.
- Valider strictement, côté serveur, tout nom de fichier fourni par un utilisateur avant d'y accéder.
- Intégrer des tests de sécurité applicative dans le cycle de développement et d'acquisition des logiciels.