

MISSION SUR LE PÉRIMÈTRE EXTERNE · GRAND GROUPE DE COMMUNICATIONS

Un périmètre externe tentaculaire, laissé ouvert par des mots de passe par défaut

Un grand groupe de télécommunications, au périmètre vaste et récemment élargi

Anonymisée avec l'accord écrit du client. Organisation, systèmes, noms d'hôtes, adresses, comptes et tout autre identifiant présents dans le rapport d'origine ont été supprimés ou généralisés. Les vulnérabilités sont décrites de manière à ne pas permettre de remonter au client.

Client	Un grand groupe de communications (anonymisé)
Mission	Test d'intrusion externe du réseau, sur un vaste parc exposé sur Internet
Approche	Approche black-box externe, exploitation non invasive, sur deux semaines environ
Testeur	Ismail Regragui, Vallum Security · OSCP, OSEP, BSCP, OSWP · Synack Red Team
Référentiels	NIST SP 800-115, OWASP Testing Guide v4.2 ; gravité selon CVSS v4.0

La demande

Mesurer la surface d'attaque externe d'un parc vaste et en forte croissance, en grande partie issu d'acquisitions récentes, et montrer quels systèmes exposés sur Internet un attaquant pouvait prendre en main sans aucun accès préalable.

Vue d'ensemble



Vulnérabilités en un coup d'œil

ID	VULNÉRABILITÉ	GRAVITÉ
1	Accès administrateur à des équipements réseau et IoT via des identifiants par défaut ou vides (plusieurs équipements)	Critique

2	Accès anonyme aux fichiers et au shell distant d'équipements réseau	Critique
3	Traversée de répertoires exposant des fichiers de configuration et des identifiants sensibles	Élevée
4	Accès administrateur à des tableaux de bord vidéo, télématiques et de gestion de bornes de recharge via des identifiants par défaut	Élevée
5	Divulgence d'identifiants et contournement d'authentification sur des routeurs grand public	Élevée
6	Failles d'exécution de code à distance connues dans des serveurs web embarqués et des logiciels réseau obsolètes	Élevée
7	Identifiants et secrets en clair exposés dans des réponses applicatives et des fichiers de configuration	Élevée
8	Tableaux de bord de supervision et bases de données chronologiques exposés sans authentification	Moyenne
9	Serveur d'intégration continue (CI) exposé, permettant une lecture de fichiers sans authentification	Moyenne
10	Partages de fichiers accessibles de façon anonyme (session nulle), révélant des informations système	Moyenne
11	Énumération de comptes sur des services de messagerie et d'accès distant	Moyenne
12	Données sensibles transmises dans les URL, et autres fuites d'informations	Moyenne
13	Identifiants d'entreprise valides récupérés dans des données de fuites publiques (OSINT)	Info

Le rapport d'origine comptait 36 vulnérabilités réparties sur de nombreux systèmes. Elles sont ici regroupées et reformulées par thème. Modèles d'équipement, noms d'hôtes, adresses, plages réseau et identifiants ont tous été retirés.

Le constat d'ensemble : deux faiblesses, répétées sur tout le parc

Plutôt qu'une seule chaîne profonde, la mission a retrouvé les deux mêmes faiblesses, encore et encore, sur un très grand périmètre.

- 1. Identifiants par défaut.** De nombreux équipements exposés sur Internet, des routeurs aux appareils spécialisés, étaient accessibles avec des identifiants d'usine ou vides, offrant un contrôle administrateur sans réel effort.
- 2. Mises à jour négligées.** De nombreux hôtes exécutaient des logiciels vieux de plusieurs années, visés par des exploits publics, dont des failles non authentifiées de divulgation d'informations et d'exécution de code à distance.
- 3. Services exposés.** Des tableaux de bord de supervision, des bases de données et des serveurs de build étaient exposés sur Internet sans authentification, divulguant des données internes et, par endroits, des identifiants

en clair.

4. **Renseignement en source ouverte.** Avant tout test, des identifiants d'entreprise valides ont été récupérés dans des données de fuites publiques — un point d'entrée tout prêt pour un attaquant.
5. **L'ampleur plutôt que la profondeur.** Avec l'accord du client, l'exploitation invasive a été volontairement limitée : la démonstration tenait au nombre de cibles faciles, non au fait d'en pousser une seule jusqu'à la compromission totale.

Le parc était inégal : certains segments étaient bien défendus — pare-feu, bannissement d'IP, arrêt automatique des services compromis — comme le notent les points forts ci-dessous.

Ce qui fonctionnait bien

- ✓ Certains segments bloquaient les outils de scan courants et détectaient les tentatives d'énumération.
- ✓ Plusieurs services compromis se sont arrêtés automatiquement, empêchant tout nouvel accès.
- ✓ Certaines parties du réseau étaient correctement cloisonnées, avec des composants à jour et des mots de passe robustes, ce qui limitait la portée d'un attaquant.

Axes de remédiation

- Éliminer les identifiants par défaut et vides sur tous les équipements exposés sur Internet, et supprimer ou placer derrière un pare-feu les services qui n'ont pas besoin d'être publics.
- Mettre en place un inventaire des actifs et une gestion des correctifs sur l'ensemble du périmètre, en particulier pour les parcs récemment acquis.
- Placer les interfaces de supervision, de base de données, de build et d'administration derrière un VPN ou une authentification, et ne jamais les exposer directement.
- Renouveler tout identifiant trouvé dans des données de fuites publiques, et déployer l'authentification multifacteur sur les services externes.

Résultat. Le client a obtenu une vue priorisée de son exposition externe sur un parc vaste et en croissance, avec une première vague de correctifs clairement identifiée (identifiants par défaut et interfaces d'administration exposées) et la recommandation de retester le périmètre régulièrement.