

MISSION WEB, API ET CLOUD · PLATEFORME DE SERVICES NUMÉRIQUES RÉGLEMENTÉE

Les données de milliers d'organisations accessibles depuis un simple compte

Une plateforme SaaS multi-tenant réglementée, hébergée sur un cloud public

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	Une plateforme de services numériques réglementée (anonymisée)
Mission	Test d'intrusion d'une application web multi-tenant, de son API et du projet cloud sous-jacent
Approche	Approche grey-box, avec des comptes peu et très privilégiés et des rôles d'audit cloud en lecture seule, sur préproduction et production, sur deux semaines environ
Testeur	Ismail Regragui, Vallum Security · OSCP, OSEP, BSCP, OSWP · Synack Red Team
Référentiels	OWASP WSTG, OWASP API Security Top 10, référentiels de sécurité cloud ; gravité selon CVSS v3.1

La demande

Déterminer si les contrôles d'accès, le cloisonnement entre clients et la configuration cloud étaient prêts pour un déploiement réglementé à grande échelle : un client pouvait-il accéder aux données d'un autre, et un utilisateur peu privilégié pouvait-il atteindre des données ou des actions réservées aux administrateurs ?

Vue d'ensemble



Vulnérabilités en un coup d'œil

ID	VULNÉRABILITÉ	GRAVITÉ
----	---------------	---------

1	Défaut d'autorisation au niveau objet (IDOR) permettant d'énumérer et de modifier les utilisateurs de toutes les organisations	Critique
2	Des utilisateurs peu privilégiés pouvaient inviter, lister et supprimer les utilisateurs d'autres organisations	Élevée
3	Accès non authentifié aux données des processus métier via l'API	Élevée
4	Cloisonnement multi-tenant insuffisant autorisant l'accès entre clients	Élevée
5	Lecture et suppression non autorisées des fichiers d'autres clients via un chemin de stockage divulgué	Élevée
6	Contournement du contrôle des téléversements autorisant des noms et des contenus de fichiers dangereux	Élevée
7	Bibliothèque de génération de documents obsolète, affectée par un déni de service connu	Élevée
8	Jetons de session non invalidés à la déconnexion	Moyenne
9	Des rôles d'audit cloud en lecture seule permettaient de télécharger des fichiers très sensibles depuis le stockage	Moyenne
10	Registre d'images cloud exposant l'architecture interne à des rôles peu privilégiés	Moyenne
11	Introspection du schéma de l'API accessible sans authentification en production	Moyenne
12	Fuite non authentifiée de la logique interne des workflows via l'API	Moyenne
13	Fuite non authentifiée d'adresses e-mail d'utilisateurs via l'API	Moyenne
14	Framework web obsolète, affecté par un contournement d'authentification connu	Moyenne
15	Clé SSH valable à l'échelle du projet cloud, sans restriction d'accès stricte	Faible
16	Bibliothèque de routage obsolète, affectée par une faille connue d'usurpation de données	Faible
17	Absence d'en-tête HTTP Strict Transport Security	Info

Vulnérabilités renumérotées et reformulées. Noms de produits, domaines, noms de projet et de stockage cloud, numéros de version précis et identité de l'entreprise énumérée ont été retirés.

Cause commune : l'autorisation décidée côté client, pas côté serveur

Les vulnérabilités les plus graves avaient une même origine : le backend se fiait aux identifiants et aux droits transmis par le client au lieu de les vérifier côté serveur.

1. **Énumérer.** Un point d'API permettait à n'importe quel utilisateur authentifié de lister toutes les organisations, exposant des milliers d'identifiants d'organisation.
2. **Pivoter.** Ces identifiants alimentaient d'autres points d'API qui ne vérifiaient pas l'appartenance : un seul compte ordinaire pouvait lire et modifier les fiches d'utilisateurs de n'importe quelle organisation, et des dizaines de milliers de fiches d'employés étaient récupérables dans la fenêtre de test.
3. **Franchir les cloisons.** Un même jeu d'identifiants était accepté sur les sous-domaines des différents clients, sans que le serveur vérifie que l'utilisateur appartenait bien à ce client — la frontière entre clients disparaissait.
4. **Atteindre le cloud.** Des messages d'erreur révélaient des chemins de stockage internes, et de simples rôles d'audit en lecture seule suffisaient pour télécharger des fichiers sensibles directement depuis le stockage cloud.
5. **Cartographier la logique.** Des requêtes API non authentifiées exposaient les définitions des workflows internes et les adresses e-mail des utilisateurs, donnant à un attaquant une vue complète du fonctionnement de la plateforme avant même toute connexion.

Un seul changement d'architecture — contrôler l'autorisation et le rattachement au client côté serveur, à chaque requête — aurait refermé d'un coup la vulnérabilité critique et la plupart des élevées.

Ce qui fonctionnait bien

- ✓ Certaines failles connues de frameworks et de bibliothèques étaient présentes au niveau des versions, mais non exploitables : l'implémentation n'exposait pas les chemins vulnérables.
- ✓ Le HTTPS était imposé sur toute la plateforme, les requêtes non sécurisées étant redirigées.
- ✓ La mission couvrait préproduction et production, ce qui a permis de confirmer les mêmes problèmes des deux côtés plutôt que de supposer leur équivalence.

Axes de remédiation

- Contrôler l'autorisation au niveau objet et au niveau fonction côté serveur, à chaque requête, à partir de l'identité et du client de l'appelant — jamais à partir d'identifiants transmis par le client.
- Désactiver l'introspection du schéma d'API en production et exiger l'authentification sur chaque requête de données.
- Resserrer l'IAM cloud pour que les rôles d'audit ne puissent pas lire les données de production, et supprimer les messages d'erreur verbeux qui révèlent les chemins de stockage.
- Invalider les jetons de session côté serveur à la déconnexion, et contrôler les fichiers dès le téléversement.

Résultat. Le rapport a fourni une feuille de route priorisée pour combler ces lacunes d'autorisation systémiques avant la montée en charge, avec une contre-vérification des correctifs et une attestation pour la conformité.