Politique de divulgation coordonnée des vulnérabilités

Introduction

Chez IDEMIA, la sécurité de nos produits et services est une priorité absolue. Nous nous engageons à maintenir les normes de sécurité les plus élevées pour protéger la vie privée et l'intégrité des données de nos clients. Nous apprécions les contributions des chercheurs en sécurité, des groupes industriels, des CERTs, des partenaires et d'autres sources pour améliorer le paysage de la sécurité. Nous nous engageons à traiter toute vulnérabilité qui est raisonnablement supposée être liée à nos produits ou services. Nous comprenons l'importance de maintenir la confidentialité de la partie rapportant et accueillons les rapports anonymes. Pour assurer la sécurité et la protection des systèmes de nos clients, nous encourageons fortement les parties rapportantes à s'engager dans une divulgation coordonnée plutôt que dans la publication immédiate des vulnérabilités au public.

En cas d'incident de sécurité potentiel, l'équipe de réponse aux incidents de sécurité des produits (PSIRT) collabore étroitement avec les ingénieurs et les équipes de développement d'IDEMIA pour élaborer un plan de réponse tout en maintenant une communication régulière avec la partie rapportante. Pour protéger la sécurité de nos produits, IDEMIA encourage la divulgation coordonnée des vulnérabilités et demande que la partie rapportante garde les informations confidentielles jusqu'à ce qu'une solution soit disponible. Notre équipe est dédiée à traiter rapidement tout problème pour assurer la fiabilité et la sécurité des produits IDEMIA.

Cette politique de divulgation de vulnérabilité coordonnée décrit le processus de signalement des vulnérabilités de sécurité à notre attention et ce que les rapporteurs peuvent attendre en retour.

Portée

Cette politique s'applique à tous les actifs numériques, produits ou services produits par IDEMIA, quel que soit leur statut en termes de statut contractuel ou de cycle de vie du produit, qu'ils soient en phase de développement, de maintenance ou même après la maintenance.

Les méthodes de test suivantes ne sont pas autorisées :

- Tests de déni de service réseau (DoS ou DDoS) ou autres tests qui entravent l'accès à un système ou endommagent des données
- Test physique (par exemple, accès aux bureaux, portes ouvertes, tailgating), ingénierie sociale (par exemple, phishing, vishing) ou tout autre test de vulnérabilité non technique.

Signalement d'une vulnérabilité

Pour signaler une vulnérabilité de sécurité, veuillez envoyer un email à psirt@idemia.com. L'email doit inclure :

- Une description détaillée de la vulnérabilité.
- Les étapes pour reproduire le problème.
- Votre évaluation de l'impact et de la gravité de la vulnérabilité. Préférablement en utilisant le CVSS v3.1 (ou v4.0)
- Un concept de preuve (PoC) ou un code d'exploitation fonctionnel, si disponible.

IDEMIA encourage la partie rapportante à crypter les informations sensibles envoyées par email.

Le PSIRT d'IDEMIA prend en charge les messages chiffrés via le logiciel de chiffrement Pretty Good Privacy (PGP)/GNU Privacy Guard (GPG). La clé publique PSIRT d'IDEMIA est disponible à l'adresse IDEMIA PSIRT Public Key.

En signalant une vulnérabilité à IDEMIA, vous acceptez qu'IDEMIA puisse utiliser librement le contenu partagé avec nous, car cette information n'est pas considérée comme propriétaire.

Lignes directrices pour la divulgation responsable

Nous vous demandons de :

- Signaler les vulnérabilités d'une manière qui minimise le risque et assure la confidentialité.
- Ne pas utiliser la vulnérabilité pour accéder, modifier, supprimer ou compromettre les données de toute autre manière.
- Nous donner un délai raisonnable pour adresser la vulnérabilité avant la divulgation publique.

Délai de réponse

Après avoir reçu votre rapport de vulnérabilité, vous pouvez vous attendre (si applicable) à :

- Un accusé de réception dans les 3 jours ouvrables (week-ends et jours fériés en France exclus).
- Une évaluation initiale et une classification de la vulnérabilité dans la semaine.
- Des mises à jour régulières sur notre progression.
- Notification de la correction de la vulnérabilité ou un calendrier pour le correctif.

Safe Harbor

IDEMIA n'engagera aucune action en justice contre les individus qui découvrent et signalent les vulnérabilités de sécurité conformément à cette politique, à condition qu'ils :

- Ne causent pas de dommage à IDEMIA, à nos clients ou à d'autres.
- Ne compromettent pas la vie privée ou la sécurité de nos clients ou le fonctionnement de nos services.
- Ne violent aucune loi criminelle.
- Divulguent publiquement les détails de la vulnérabilité uniquement après qu'IDEMIA a confirmé l'achèvement des efforts de remédiation.

Reconnaissance

Nous reconnaîtrons publiquement votre contribution, à moins que vous ne préfériez rester anonyme. Bien que nous n'offrions pas de programme de bug bounty ou d'autre compensation, nous reconnaissons et apprécions les contributions des chercheurs en sécurité.

Modifications de cette politique

IDEMIA se réserve le droit de modifier cette politique à tout moment sans préavis. Nous vous encourageons à visiter régulièrement cette page pour toute mise à jour.