Coordinated Vulnerability Disclosure policy

Introduction

At IDEMIA, the security of our products and services is a top priority. We are dedicated to upholding the highest standards of security to safeguard the privacy and integrity of our customers' data. We value the contributions of security researchers, industry groups, CERTs, partners, and other sources in enhancing the security landscape. We are committed to addressing any vulnerability that is reasonably believed to be related to our products or services. We understand the importance of maintaining the confidentiality of the reporting party and welcome anonymous reports. To ensure the safety and security of our customers' systems, we strongly encourage reporting parties to engage in coordinated disclosure, rather than immediate public release of vulnerabilities.

In the event of a potential security incident, the Product Security Incident Response Team (PSIRT) collaborates closely with IDEMIA's engineers and development teams to formulate a response plan, while maintaining regular communication with the reporting party. To safeguard the security of our products, IDEMIA encourages coordinated disclosure of vulnerabilities and requests that the reporting party keep the information confidential until a resolution is available. Our team is dedicated to promptly addressing any issues to ensure the reliability and security of IDEMIA products.

This Coordinated Vulnerability Disclosure Policy outlines the process for reporting security vulnerabilities to us and what reporters can expect in return.

Scope

This Policy applies to all digital assets, products, or services produced by IDEMIA, regardless of their status in terms of contractual status or the product lifecycle-whether they are in the stages of development, maintenance, or even post-maintenance.

The following test methods are not authorized:

- Network denial of service (DoS or DDoS) tests or other tests that impair access to or damage a system or data
- Physical testing (e.g. office access, open doors, tailgating), social engineering (e.g. phishing, vishing), or any other non-technical vulnerability testing

Reporting a Vulnerability

To report a security vulnerability, please send an email to psirt@idemia.com. The email should include:

- A detailed description of the vulnerability.
- Steps to reproduce the issue.
- Your assessment of the impact and severity of the vulnerability. Preferably by using the CVSS v3.1 (or v4.0)
- Proof-of-Concept (PoC) or working exploit code, if available.

IDEMIA encourages the reporting party to encrypt sensitive information sent via email. The IDEMIA PSIRT supports encrypted messages via Pretty Good Privacy (PGP)/GNU Privacy Guard (GPG) encryption software. The IDEMIA PSIRT public key is available at IDEMIA PSIRT Public Key.

By reporting a vulnerability to IDEMIA, you agree that IDEMIA can freely use the content shared with us, as this information is not considered proprietary.

Responsible Disclosure Guidelines

We ask that you:

- Report vulnerabilities in a manner that minimizes risk and ensures confidentiality.
- Do not use the vulnerability to access, modify, delete, or otherwise compromise data.
- Provide us with a reasonable amount of time to address the vulnerability before public disclosure.

Response Timeline

Upon receiving your vulnerability report, you can expect (if applicable):

- An acknowledgment of receipt within 3 working days (excluding weekends and public holidays in France).
- An initial assessment and classification of the vulnerability within one week.
- Regular updates on our progress.
- Notification of the vulnerability remediation or a timeline for the fix.

Safe Harbor

IDEMIA will not engage any legal action against individuals who discover and report security vulnerabilities in accordance with this policy provided they:

- Do not cause harm to IDEMIA, our customers, or others.
- Do not compromise the privacy or safety of our customers or the operation of our services.
- Do not violate any criminal laws.
- Publicly disclose vulnerability details only after IDEMIA has confirmed the completion of remediation efforts.

Recognition

We will publicly acknowledge your contribution unless you prefer to remain anonymous. While we do not offer a bug bounty program or any other compensation, we do recognize and appreciate the contributions of security researchers.

Modifications to This Policy

IDEMIA reserves the right to modify this policy at any time without notice. We encourage you to regularly visit this page for any updates.