DJ-CERT
Centre national de veille, d'alerte et de réponse aux attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 24-05-2025

BULLETIN ALERTES

Object	Vulnérabilité dans OpenPGP.js library
Réference	1351
Date de Publication	2025-05-23
Sévérité	Critique

IMPACT :

- Accès aux informations confidentielles
- Porter atteinte à la confidentialité de données
- Usurpation d'identité

SYSTÉME AFFECTÉ :

- OpenPGP.js library versions v5 antérieures à 5.11.3
- OpenPGP.js library versions v6 antérieures à 6.1.1

DÉSCRIPTION :

Une vulnérabilité critique a été découverte dans « OpenPGP.js », une bibliothèque JavaScript largement utilisée pour le chiffrement de bout en bout dans les applications web. Cette vulnérabilité permet à un attaquant de contourner les mécanismes de vérification des signatures numériques, rendant possible la falsification de messages signés ou signés et chiffrés. Son exploitation peut entraîner une usurpation d'identité ainsi qu'une atteinte à l'intégrité et à la confidentialité des données.

SOLUTION :

Mettre à jour OpenPGP.js.(se référer à la documentation)

DOCUMENTATION :

- Bulletin de sécurité OpenPGP.js:

https://github.com/openpgpjs/openpgpjs/security/advisories/GHSA-8qff-qr5q-5pr8

- CVE-2025-47934:https://nvd.nist.gov/vuln/detail/CVE-2025-47934