



BULLETIN DE SECURITE

Titre	Vulnérabilités critiques dans OpenPGP.js library
Numéro de Référence	54702305/25
Date de Publication	23 Mai 2025
Risque	Critique
Impact	Critique

Systemes affectés

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

Identificateurs externes

- CVE-2025-47934

Bilan de la vulnérabilité

Une vulnérabilité critique a été identifiée 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 la vérification des signatures numériques, rendant possible la falsification des messages signés en ligne ou signés et chiffrés. L'exploitation de cette faille peut conduire à une usurpation d'identité, à une atteinte à l'intégrité et la confidentialité des données.

Solution

Veillez se référer au bulletin de sécurité OpenPGP.js, afin d'installer les nouvelles mises à jour.

Risque

- Accès aux informations confidentielles,
- Porter atteinte à la confidentialité de données,

- Usurpation d'identité,

Référence

Bulletin de sécurité OpenPGP.js:

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