مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Signature Spoofing Flaw in OpenPGP.js

Tracking #:432317298

Date:23-05-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability has been identified in OpenPGP.js, an open-source JavaScript library widely used to enable end-to-end encryption in web applications.

TECHNICAL DETAILS:

A critical vulnerability (CVE-2025-47934) has been identified in OpenPGP.js, an open-source JavaScript library widely used to enable end-to-end encryption in web applications. This flaw allows attackers to spoof digital signatures on inline-signed and signed+encrypted messages, making tampered content appear as if it were legitimately signed by a trusted sender.

Technical Details

- **CVE ID:** CVE-2025-47934
- **Severity**: Critical
- **Impact Type:** Signature Spoofing / Message Integrity Compromise
- **Vulnerable Functionality:**
  - openpgp.verify() (inline signed messages)
  - openpgp.decrypt() with verificationKeys (signed+encrypted messages)
- **Affected versions**: 5.0.1 - 5.11.2 || 6.0.0-alpha.0 - 6.1.0. OpenPGP.js v4 is not affected.
- **Patched versions**: 5.11.3, 6.1.1
- **Workarounds**
  - When verifying inline-signed messages, extract the message and signature(s) from the message returned by openpgp.readMessage, and verify the(/each) signature as a detached signature by passing the signature and a new message containing only the data (created using openpgp.createMessage) to openpgp.verify.
  - When decrypting and verifying signed+encrypted messages, decrypt and verify the message in two steps, by first calling openpgp.decrypt without verificationKeys, and then passing the returned signature(s) and a new message containing the decrypted data (created using openpgp.createMessage) to openpgp.verify.

RECOMMENDATIONS:

- Update OpenPGP.js immediately to patched version.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

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