Crypt::SecretBuffer versions before 0.019 for Perl is suseceptible to timing attacks

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-5086
State	PUBLISHED
Assigner	CPANSec
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-13 23:16:27 UTC
Updated	2026-04-14 02:16:05 UTC
Description	Crypt::SecretBuffer versions before 0.019 for Perl is suseceptible to timing attacks. For example, if Crypt::SecretBuffer was

Risk And Classification

Problem Types: CWE-208 | CWE-208 CWE-208 Observable Timing Discrepancy

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	NERDVANA	CryptSecretBuffer	affected 0.019 custom	Not specified

References

Reference	Source	Link
www.openwall.com/lists/oss-security/2026/04/13/12	af854a3a-2127-422b-91ae-364da2661108	www.openwall.c
metacpan.org/release/NERDVANA/Crypt-SecretBuffer-0.019/source/Changes	9b29abf9-4ab0-4765-b253-1875cd9b441e	metacpan.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Solutions

CNA: Upgrade to version 0.019 or later.

There are currently no legacy QID mappings associated with this CVE.