CryptX versions before 0.088 for Perl do not reseed the Crypt::PK PRNG state after forking

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

Summary

CVE	CVE-2026-41564
State	PUBLISHED
Assigner	CPANSec
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-23 08:16:01 UTC
Updated	2026-04-23 10:16:17 UTC
Description	CryptX versions before 0.088 for Perl do not reseed the Crypt::PK PRNG state after forking. The Crypt::PK::RSA, Crypt::PK

Risk And Classification

Problem Types: CWE-335 | CWE-338 | CWE-335 CWE-335 Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG) | CWE-338 CWE-338 Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	MIK	CryptX	affected 0.088 custom	Not specified

References

Reference	Source	Link
github.com/DCIT/perl-CryptX/commit/9a1dd3e0c27d68e32450be5538b864c2b115e...	9b29abf9-4ab0-4765-b253-1875cd9b441e	github.c
metacpan.org/release/MIK/CryptX-0.088	9b29abf9-4ab0-4765-b253-1875cd9b441e	metacpa
www.openwall.com/lists/oss-security/2026/04/23/2	af854a3a-2127-422b-91ae-364da2661108	www.op
github.com/DCIT/perl-CryptX/security/advisories/GHSA-24c2-gp6c-24c6	9b29abf9-4ab0-4765-b253-1875cd9b441e	github.c
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
CNA	2026-04-18T00:00:00.000Z	Issue discovered.
CNA	2026-04-21T00:00:00.000Z	Reported to upstream maintainer.
CNA	2026-04-23T00:00:00.000Z	CryptX 0.088 released with fix.

Solutions

CNA: Upgrade to CryptX 0.088 or later, or apply the upstream patch. Applying the fix does not retroactively protect keys that may already have been exposed. On an affected version, any private key used with or generated by a Crypt::PK::* object created before `fork()` should be assessed for rotation.

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