Amazon::Credentials versions through 1.2.0 for Perl uses rand to generate encryption keys

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

Summary

CVE	CVE-2026-6146
State	PUBLISHED
Assigner	CPANSec
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-11 20:25:47 UTC
Updated	2026-05-12 16:48:58 UTC
Description	Amazon::Credentials versions through 1.2.0 for Perl uses rand to generate encryption keys. Amazon::Credentials stores cre

Risk And Classification

EPSS: 0.000130000 probability, percentile 0.019970000 (date 2026-05-12)

Problem Types: CWE-338 | CWE-338 CWE-338 Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	BIGFOOT	AmazonCredentials	affected 1.2.0 custom	Not specified

References

Reference	Source	Link
www.openwall.com/lists/oss-security/2026/05/11/15	af854a3a-2127-422b-91ae-364da2661108	www.open
metacpan.org/release/BIGFOOT/Amazon-Credentials-1.2.0/source/lib/Amazon/Cr...	9b29abf9-4ab0-4765-b253-1875cd9b441e	metacpan.
metacpan.org/release/BIGFOOT/Amazon-Credentials-1.3.0/changes	9b29abf9-4ab0-4765-b253-1875cd9b441e	metacpan.
CVE Program record	CVE.ORG	www.cve.c
NVD vulnerability detail	NVD	nvd.nist.gc

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Solutions

CNA: Upgrade to version 1.3.0 or later.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**