Crypt::PasswdMD5 versions through 1.42 for Perl generates insecure random values for salts

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

Summary

CVE	CVE-2026-6659
State	PUBLISHED
Assigner	CPANSec
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-08 18:16:34 UTC
Updated	2026-05-12 16:45:18 UTC
Description	Crypt::PasswdMD5 versions through 1.42 for Perl generates insecure random values for salts. The built-in rand function is p

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from ADP

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

EPSS: 0.000110000 probability, percentile 0.014150000 (date 2026-05-12)

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

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

None

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	RSAVAGE	CryptPasswdMD5	affected 1.42 custom	Not specified

References

Reference	Source	Link
metacpan.org/release/RSAVAGE/Crypt-PasswdMD5-1.42/source/lib/Crypt/PasswdM...	9b29abf9-4ab0-4765-b253-1875cd9b441e	metacp
www.openwall.com/lists/oss-security/2026/05/08/17	af854a3a-2127-422b-91ae-364da2661108	www.op
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nis

No vendor comments have been submitted for this CVE.

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