



Apache::API::Password versions through v0.5.2 for Perl can generate insecure random values for salts

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-5088
State	PUBLISHED
Assigner	CPANSec
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-15 08:16:16 UTC
Updated	2026-04-15 18:17:24 UTC
Description	Apache::API::Password versions through v0.5.2 for Perl can generate insecure random values for salts. The <code>_make_salt</code> ar

Risk And Classification

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	JDEGUEST	ApacheAPIPassword	affected v0.5.2 custom	Not specified

References

Reference	Source	Link
metacpan.org/release/JDEGUEST/Apache2-API-v0.5.2/view/lib/Apache2/API/Pass...	9b29abf9-4ab0-4765-b253-1875cd9b441e	metacpan
security.metacpan.org/docs/guides/random-data-for-security.html	9b29abf9-4ab0-4765-b253-1875cd9b441e	security.r
metacpan.org/pod/Crypt::URandom	9b29abf9-4ab0-4765-b253-1875cd9b441e	metacpan
metacpan.org/release/JDEGUEST/Apache2-API-v0.5.3/changes	9b29abf9-4ab0-4765-b253-1875cd9b441e	metacpan
www.openwall.com/lists/oss-security/2026/04/15/4	af854a3a-2127-422b-91ae-364da2661108	www.ope
www.openwall.com/lists/oss-security/2026/04/15/5	af854a3a-2127-422b-91ae-364da2661108	www.ope
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Solutions

CNA: Upgrade to version v0.5.3 or later, and install Crypt::URandom.

Workarounds

CNA: Install Crypt::URandom.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)