Apache::Session::Generate::MD5 versions through 1.94 for Perl create insecure session id

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

Summary

CVE	CVE-2025-40931
State	PUBLISHED
Assigner	CPANSec
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-05 02:16:39 UTC
Updated	2026-04-12 18:16:38 UTC
Description	Apache::Session::Generate::MD5 versions through 1.94 for Perl create insecure session id. Apache::Session::Generate::M

Risk And Classification

Primary CVSS: v3.1 9.1 CRITICAL from ADP

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

Problem Types: CWE-338 | CWE-340 | CWE-340 CWE-340 Generation of Predictable Numbers or Identifiers | CWE-338 CWE-338 Use of Cryptographically Weak Pseudo-Random Number Generator

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Chorny	Apache	\	session\	\	generate\

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	CHORNY	ApacheSessionGenerateMD5	affected 1.94 custom	Not specified

References

Reference	Source	Link
salsa.debian.org/perl-team/modules/packages/libapache-session-perl/-/commit/bd...	9b29abf9-4ab0-4765-b253-1875cd9b441e	salsa.debi
gitlab.ow2.org/lemonldap-ng/lemonldap-ng/-/work_items/1633	9b29abf9-4ab0-4765-b253-1875cd9b441e	gitlab.ow2
metacpan.org/pod/Apache::Session::Generate::Random	9b29abf9-4ab0-4765-b253-1875cd9b441e	metacpan
www.openwall.com/lists/oss-security/2019/06/15/1	9b29abf9-4ab0-4765-b253-1875cd9b441e	www.oper
github.com/chorny/Apache-Session/issues/4	9b29abf9-4ab0-4765-b253-1875cd9b441e	github.cor
security.metacpan.org/docs/guides/random-data-for-security.html	9b29abf9-4ab0-4765-b253-1875cd9b441e	security.m
metacpan.org/dist/Apache-Session/source/lib/Apache/Session/Generate/MD5.pm	9b29abf9-4ab0-4765-b253-1875cd9b441e	metacpan
www.openwall.com/lists/oss-security/2026/03/05/3	af854a3a-2127-422b-91ae-364da2661108	www.oper
bugs.debian.org/cgi-bin/bugreport.cgi	9b29abf9-4ab0-4765-b253-1875cd9b441e	bugs.debi
rt.cpan.org/Ticket/Display.html	9b29abf9-4ab0-4765-b253-1875cd9b441e	rt.cpan.org
CVE Program record	CVE.ORG	www.cve.c
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
CNA	2017-10-06T00:00:00.000Z	Issue created in the GitHub repository for Apache-Session identifying poor entropy.
CNA	2019-06-15T00:00:00.000Z	Report posted to the Open Source Security mailing list.
CNA	2019-06-17T00:00:00.000Z	Debian bug 930659 for libapache-session-perl poor source of entropy for session id generation

CNA	2019-06-20T00:00:00.000Z	Patch to use Crypt::URandom created by the Debian Perl Group.
CNA	2025-09-04T00:00:00.000Z	Issue reported to CPANSec.
CNA	2026-03-05T00:00:00.000Z	CVE disclosed by CPANSec.

Solutions

CNA: Consider alternate solutions like https://metacpan.org/pod/Apache::Session::Generate::Random

Workarounds

CNA: Apply the patch from the Debian Perl Group that uses 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 registred 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**