Apache::Session::Generate::ModUniqueId versions from 1.54 through 1.94 for Perl session ids are insecure

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

Summary

CVE	CVE-2026-5081
State	PUBLISHED
Assigner	CPANSec
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-06 13:16:09 UTC
Updated	2026-05-07 14:52:27 UTC
Description	Apache::Session::Generate::ModUniqueId versions from 1.54 through 1.94 for Perl session ids are insecure. Apache::Sess

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

EPSS: 0.000380000 probability, percentile 0.114770000 (date 2026-05-12)

Problem Types: CWE-340 | CWE-340 CWE-340 Generation of Predictable Numbers or Identifiers

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

Integrity

High

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	CHORNY	ApacheSessionGenerateModUniqueId	affected 1.54 1.94 custom	Not specified

References

Reference	Source	Link	Tags
httpd.apache.org/docs/current/mod/mod_unique_id.html	9b29abf9-4ab0-4765-b253-1875cd9b441e	httpd.apache.org	
metacpan.org/pod/Apache::Session::Generate::Random	9b29abf9-4ab0-4765-b253-1875cd9b441e	metacpan.org	
www.openwall.com/lists/oss-security/2026/05/06/6	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analy

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Solutions

CNA: In cases where the session id is used for authentication or provides access to restricted data, consider alternate solutions like Apache::Session::Generate::Random.

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