



# 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 !\[\]\(666e09182d4cd268646ea700ea60dcdf\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2026-5081
<b>State</b>	PUBLISHED
<b>Assigner</b>	CPANSec
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-06 13:16:09 UTC
<b>Updated</b>	2026-05-07 14:52:27 UTC
<b>Description</b>	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
<a href="httpd.apache.org/docs/current/mod/mod_unique_id.html">httpd.apache.org/docs/current/mod/mod_unique_id.html</a>	9b29abf9-4ab0-4765-b253-1875cd9b441e	<a href="httpd.apache.org">httpd.apache.org</a>	
<a href="metacpan.org/pod/Apache::Session::Generate::Random">metacpan.org/pod/Apache::Session::Generate::Random</a>	9b29abf9-4ab0-4765-b253-1875cd9b441e	<a href="metacpan.org">metacpan.org</a>	
<a href="www.openwall.com/lists/oss-security/2026/05/06/6">www.openwall.com/lists/oss-security/2026/05/06/6</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="www.openwall.com">www.openwall.com</a>	
CVE Program record	CVE.ORG	<a href="www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="nvd.nist.gov">nvd.nist.gov</a>	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.

© 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](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)