



# HTTP::Session versions through 0.53 for Perl defaults to using insecurely generated session ids

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

## Summary

<b>CVE</b>	CVE-2026-3256
<b>State</b>	PUBLISHED
<b>Assigner</b>	CPANSec
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-28 19:16:56 UTC
<b>Updated</b>	2026-04-01 15:23:23 UTC
<b>Description</b>	HTTP::Session versions through 0.53 for Perl defaults to using insecurely generated session ids. HTTP::Session defaults to

## Risk And Classification

**Primary CVSS:** v3.1 9.8 CRITICAL from nvd@nist.gov

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

**EPSS:** 0.000160000 probability, percentile 0.036110000 (date 2026-04-01)

**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	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	ADP	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ktat	Http	\	session	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	KTAT	HTTPSession	affected 0.53 custom	Not specified

### References

Reference	Source	Link
metacpan.org/release/KTAT/http-session-0.53/source/lib/HTTP/Session/ID/SHA...	9b29abf9-4ab0-4765-b253-1875cd9b441e	metacpan
metacpan.org/release/KTAT/http-session-0.53/source/lib/HTTP/Session/ID/MD5.pm	9b29abf9-4ab0-4765-b253-1875cd9b441e	metacpan
www.openwall.com/lists/oss-security/2026/03/28/5	af854a3a-2127-422b-91ae-364da2661108	www.oper
security.metacpan.org/docs/guides/random-data-for-security.html	9b29abf9-4ab0-4765-b253-1875cd9b441e	security.m
CVE Program record	CVE.ORG	www.cve.r
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

### Additional Advisory Data

#### Workarounds

**CNA:** Users on systems with a /dev/urandom device should configure the module to use HTTP::Session::ID::Urandom. Users on systems without a /dev/urandom (such as Windows) device will need to create custom ID modules that make use of module such as Crypt::SysRandom or 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](#).

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