



# Catalyst::Plugin::Statsd versions through 0.10.0 for Perl may leak session ids

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

## Summary

<b>CVE</b>	CVE-2026-45180
<b>State</b>	PUBLISHED
<b>Assigner</b>	CPANSec
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-10 21:16:29 UTC
<b>Updated</b>	2026-05-10 21:16:29 UTC
<b>Description</b>	Catalyst::Plugin::Statsd versions through 0.10.0 for Perl may leak session ids. If the communication channel to the statsd d...

## Risk And Classification

**Problem Types:** CWE-319 | CWE-319 CWE-319 Cleartext Transmission of Sensitive Information

## Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	RRWO	CatalystPluginStatsd	affected 0.10.0 custom	Not specified

## References

Reference	Source	Link
github.com/robrwo/Plack-Middleware-Statsd/security/advisories/GHSA-9gwm-...	9b29abf9-4ab0-4765-b253-1875cd9b441e	<a href="#">github.com</a>
metacpan.org/release/RRWO/Catalyst-Plugin-Statsd-v0.10.0/changes	9b29abf9-4ab0-4765-b253-1875cd9b441e	<a href="#">metacpan.org</a>
github.com/robrwo/CatalystX-Statsd/security/advisories/GHSA-gjvr-hq83-fc38	9b29abf9-4ab0-4765-b253-1875cd9b441e	<a href="#">github.com</a>
www.cve.org/CVERecord	9b29abf9-4ab0-4765-b253-1875cd9b441e	<a href="#">www.cve.org</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Additional Advisory Data

### Solutions

**CNA:** Upgrade to version 0.10.0 or later, which will no longer log session ids to statsd. If Plack::Middleware::Statsd is upgraded to 0.9.0 or later and is configured to log some information securely, then session ids will be logged as HMAC signatures instead.

#### Workarounds

**CNA:** Use a statsd daemon on the same host or through a secure communications channel.

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](#)