Net::Statsd::Lite versions through 0.10.0 for Perl allowed metric injections

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

Summary

CVE	CVE-2026-8788
State	PUBLISHED
Assigner	CPANSec
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-18 08:16:15 UTC
Updated	2026-05-18 08:16:15 UTC
Description	Net::Statsd::Lite versions through 0.10.0 for Perl allowed metric injections. The values from the set_add method were not cl

Risk And Classification

Problem Types: CWE-93 | CWE-93 CWE-93 Improper Neutralization of CRLF Sequences

Vendor Declared Affected Products

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

References

Reference	Source	Link	Tags
www.cve.org/CVERecord	9b29abf9-4ab0-4765-b253-1875cd9b441e	www.cve.org	
metacpan.org/release/RRWO/Net-Statsd-Lite-v0.10.1/changes	9b29abf9-4ab0-4765-b253-1875cd9b441e	metacpan.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ana

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
CNA	2026-05-14T00:00:00.000Z	Issue reported to CPANSec
CNA	2026-05-15T00:00:00.000Z	Author notified
CNA	2026-05-16T00:00:00.000Z	Fix released for CVE-2026-46719

CNA	2026-05-17T00:00:00.000Z	CVE-2026-8788 identified by author
CNA	2025-05-17T00:00:00.000Z	Fix released for CVE-2026-8788

Solutions

CNA: Upgrade to Net::Statsd::Lite version 0.10.1 or later.

Workarounds

CNA: In version 0.10.0, use the secure_set_add method which logs an HMAC digest of the value instead of the raw value. Validate that all values sent to the client based on untrusted data do not contain metric injections.

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