Plack::Middleware::Session::Cookie versions through 0.21 for Perl allows remote code execution

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

Summary

CVE	CVE-2014-125112
State	PUBLISHED
Assigner	CPANSec
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-26 03:16:00 UTC
Updated	2026-05-06 14:50:24 UTC
Description	Plack::Middleware::Session::Cookie versions through 0.21 for Perl allows remote code execution. Plack::Middleware::Sessi

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from ADP

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

Problem Types: CWE-565 | CWE-565 CWE-565 Reliance on Cookies without Validation and Integrity Checking

Version	Source	Type	Score	Severity	Vector
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

ntegrity

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	Miyagawa	Plack	\	middleware\	\	session\

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	MIYAGAWA	PlackMiddlewareSessionCookie	affected 0.21 custom	Not specified

References

Reference	Source	Link
www.openwall.com/lists/oss-security/2026/03/26/2	af854a3a-2127-422b-91ae-364da2661108	www.open
gist.github.com/miyagawa/2b8764af908a0dacd43d	9b29abf9-4ab0-4765-b253-1875cd9b441e	gist.github
metacpan.org/release/MIYAGAWA/Plack-Middleware-Session-0.23-TRIAL/changes	9b29abf9-4ab0-4765-b253-1875cd9b441e	metacpan.
CVE Program record	CVE.ORG	www.cve.c
NVD vulnerability detail	NVD	nvd.nist.gc

Vendor Comments And Credit

Discovery Credit

CNA: mala (@bulkneets) (en)

Additional Advisory Data

Source	Time	Event
CNA	2014-08-11T00:00:00.000Z	Vulnerability disclosed by MIYAGAWA.
CNA	2014-08-11T00:00:00.000Z	Version 0.22 released that warns when the "secret" option is not set.
CNA	2014-08-11T00:00:00.000Z	Version 0.23-TRIAL released that requires the "secret" option to be set.
CNA	2014-09-05T00:00:00.000Z	Version 0.24 released. Same as 0.23 but not a trial release.
CNA	2016-02-03T00:00:00.000Z	Version 0.26 released. Documentation improved with SYNOPSIS giving an example of how to set the
CNA	2019-01-26T00:00:00.000Z	CPANSA-Plack-Middleware-Session-Cookie-2014-01 assigned in CPAN::Audit::DB
CNA	2019-03-09T00:00:00.000Z	CPANSA-Plack-Middleware-Session-2014-01 reassigned in CPAN::Audit::DB
CNA	2025-07-08T00:00:00.000Z	CVE-2014-125112 assigned by CPANSec.

Solutions

CNA: Upgrade Plack::Middleware::Session to version 0.23 or later (ideally version 0.36 or later), and set the "secret" option.

Workarounds

CNA: Set the "secret" option.

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