Plack::Middleware::XSendfile versions through 1.0053 for Perl can allow client-controlled path rewriting

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

Summary

CVE	CVE-2026-7381
State	PUBLISHED
Assigner	CPANSec
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-29 23:16:19 UTC
Updated	2026-04-29 23:16:19 UTC
Description	Plack::Middleware::XSendfile versions through 1.0053 for Perl can allow client-controlled path rewriting. Plack::Middleware:

Risk And Classification

Problem Types: CWE-200 | CWE-441 | CWE-913 | CWE-200 CWE-200 Exposure of Sensitive Information to an Unauthorized Actor | CWE-441 CWE-441 Unintended Proxy or Intermediary | CWE-913 CWE-913 Improper Control of Dynamically-Managed Code Resources

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	MIYAGAWA	PlackMiddlewareXSendfile	affected 1.0053 custom	Not specified

References

Reference	Source	Link
metacpan.org/release/MIYAGAWA/Plack-1.0053/view/lib/Plack/Middleware/XSend...	9b29abf9-4ab0-4765-b253-1875cd9b441e	metacpar
metacpan.org/release/MIYAGAWA/Plack-1.0053/changes	9b29abf9-4ab0-4765-b253-1875cd9b441e	metacpar
nvd.nist.gov/vuln/detail/CVE-2025-61780	9b29abf9-4ab0-4765-b253-1875cd9b441e	nvd.nist.g
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

Vendor Comments And Credit

Discovery Credit

CNA: CPANSec (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-10-10T00:00:00.000Z	Issue for Rack::Sendfile reported
CNA	2026-04-27T00:00:00.000Z	Issue reported to maintainer of Plack
CNA	2025-04-28T00:00:00.000Z	Plack 1.0052 released with improved security documentation in Plack::Middleware::XSendfile
CNA	2025-04-29T00:00:00.000Z	Plack 1.0053 released that deprecates Plack::Middleware::XSendfile

Solutions

CNA: Users are encouraged to set the appropriate header directly in their applications, or write their own middleware layer that does not allow configuration to be passed via HTTP request headers.

Workarounds

CNA: Users can configure the X-Sendfile-Type in the middleware constructor, and the reverse proxy to unset the X-Sendfile-Type header and (on nginx) the X-Accel-Mapping request header.

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