



Starlet versions through 0.31 for Perl allows HTTP Request Smuggling via Improper Header Precedence

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

Summary

CVE	CVE-2026-40561
State	PUBLISHED
Assigner	CPANSec
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-03 01:15:58 UTC
Updated	2026-05-03 05:15:58 UTC
Description	Starlet versions through 0.31 for Perl allows HTTP Request Smuggling via Improper Header Precedence. Starlet incorrectly

Risk And Classification

Problem Types: CWE-444 | CWE-444 CWE-444 Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	KAZUHO	Starlet	affected 0.31 custom	Not specified

References

Reference	Source	Link
datatracker.ietf.org/doc/html/rfc7230	9b29abf9-4ab0-4765-b253-1875cd9b441e	datatracker
github.com/kazuho/Starlet/commit/a7d5dfd1862aafa43e5eaca0fdb6acf4cc15b2d...	9b29abf9-4ab0-4765-b253-1875cd9b441e	github.com
www.openwall.com/lists/oss-security/2026/05/03/1	af854a3a-2127-422b-91ae-364da2661108	www.openw
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go

Vendor Comments And Credit

Discovery Credit

CNA: CPANSec (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-04-12T00:00:00.000Z	Issue identified
CNA	2026-04-28T00:00:00.000Z	Maintainer notified
CNA	2026-05-02T00:00:00.000Z	Determined that the issue was already public on GitHub

Workarounds

CNA: Migrate to Starman 0.4018 or later which has fixed this issue or apply the patch.

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](#)