Request smuggling via first-wins Content-Length parsing in inets httpd

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-23941
State	PUBLISHED
Assigner	EEF
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-13 19:54:15 UTC
Updated	2026-04-06 17:17:08 UTC
Description	Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in Erlang OTP (inets httpd module)

Risk And Classification

Primary CVSS: v4.0 7 HIGH from 6b3ad84c-e1a6-4bf7-a703-f496b71e49db

CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:N/VI:N/VA:N/SC:H/SI:H/SA:L/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

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

Version	Source	Type	Score	Severity	Vector
4.0	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	Secondary	7	HIGH	CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:N/VI:N/VA:
4.0	CNA	CVSS	7	HIGH	CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:N/VI:N/VA:

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

Present

Privileges Required

None

User Interaction

None

Confidentiality

None

ntegrity

None

Availability

None

Sub Conf.

High

Sub Integrity

High

Sub Availability

Low

CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:N/VI:N/VA:N/SC:H/SI:H/SA:L/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Erlang	OTP	affected 5.10 * otp	Not specified
CNA	Erlang	OTP	affected 17.0 * otp	Not specified
CNA	Erlang	OTP	affected * git	Not specified

References

Reference	Source	Link
github.com/erlang/otp/commit/a4b46336fd25aa100ac602eb9a627aaead7eda18	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	github.com
cna.erlef.org/cves/CVE-2026-23941.html	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	cna.erlef.org
www.erlang.org/doc/system/versions.html	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	www.erlang.or
github.com/erlang/otp/security/advisories/GHSA-w4jc-9wpv-pqh7	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	github.com
github.com/erlang/otp/commit/a761d391d8d08316cbd7d4a86733ba932b73c45b	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	github.com
osv.dev/vulnerability/EEF-CVE-2026-23941	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	osv.dev
github.com/erlang/otp/commit/e775a332f623851385ab6ddb866d9b150612ddf6	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Luigino Camastra / Aisle Research (en)

CNA: Konrad Pietrzak (en)

Additional Advisory Data

Workarounds

CNA: * Configure frontend proxy to reject requests with duplicate Content-Length headers. * Disable HTTP keep-alive on httpd by adding `{keep_alive, false}` to httpd configuration. Note: This impacts performance for clients making multiple requests. * Deploy a Web Application Firewall (WAF) configured to reject requests with multiple Content-Length headers.

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