



Request smuggling due to acceptance of invalid chunked data in net/http

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

Summary

CVE	CVE-2025-22871
State	PUBLISHED
Assigner	Go
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-04-08 20:15:20 UTC
Updated	2026-05-12 13:16:39 UTC
Description	The net/http package improperly accepts a bare LF as a line terminator in chunked data chunk-size lines. This can permit re

Risk And Classification

Primary CVSS: v3.1 9.1 CRITICAL from ADP

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

EPSS: 0.003420000 probability, percentile 0.568870000 (date 2026-05-12)

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

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Go Standard Library	Net/http/internal	affected 1.23.8 semver	Not specified
CNA	Go Standard Library	Net/http/internal	affected 1.24.0-0 1.24.2 semver	Not specified
ADP	Siemens	SENTRON 7KT PAC1261 Data Manager	affected V2.1.0 custom	Not specified

References

Reference	Source	Link	Tags
go.dev/issue/71988	security@golang.org	go.dev	
cert-portal.siemens.com/productcert/html/ssa-783943.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.com	
pkg.go.dev/vuln/GO-2025-3563	security@golang.org	pkg.go.dev	
groups.google.com/g/golang-announce/c/Y2uBTVKjBQk	security@golang.org	groups.google.com	
go.dev/cl/652998	security@golang.org	go.dev	
www.openwall.com/lists/oss-security/2025/04/04/4	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

Vendor Comments And Credit

Discovery Credit

CNA: [Jeppe Bonde Weikop \(en\)](#)

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