Infinite loop in HTTP/2 transport when given bad SETTINGS_MAX_FRAME_SIZE in net/http/internal/http2 in golang.org/x/net

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

Summary

CVE	CVE-2026-33814
State	PUBLISHED
Assigner	Go
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-07 20:16:42 UTC
Updated	2026-05-08 19:16:30 UTC
Description	When processing HTTP/2 SETTINGS frames, transport will enter an infinite loop of writing CONTINUATION frames if it rec

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from ADP

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

EPSS: 0.000190000 probability, percentile 0.052630000 (date 2026-05-11)

Problem Types: CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop')

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

ntegrity

None

vailability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Golang.orgxnet	Golang.org/x/net/http2	affected 0.53.0 semver	Not specified
CNA	Go Standard Library	Net/http	affected 1.25.10 semver	Not specified
CNA	Go Standard Library	Net/http	affected 1.26.0-0 1.26.3 semver	Not specified

References

Reference	Source	Link	Tags
go.dev/issue/78476	security@golang.org	go.dev	
go.dev/cl/761581	security@golang.org	go.dev	
go.dev/cl/761640	security@golang.org	go.dev	
groups.google.com/g/golang-announce/c/qcCIEXso47M	security@golang.org	groups.google.com	
pkg.go.dev/vuln/GO-2026-4918	security@golang.org	pkg.go.dev	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Marwan Atia (marwansamir688@gmail.com) (en)

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