HTTP Request Smuggling in visualfc/liteide

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

Summary

CVE	CVE-2026-4742
State	PUBLISHED
Assigner	GovTech CSG
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-24 04:17:30 UTC
Updated	2026-05-05 20:38:41 UTC
Description	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling') vulnerability in visualfc liteide (liteide>

Risk And Classification

Primary CVSS: v4.0 2.9 LOW from cve_disclosure@tech.gov.sg

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:L/SI:L/SA:N/E:P/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:N/AU:N/R:U/V:D/RE:L/U:Green

EPSS: 0.000600000 probability, percentile 0.185670000 (date 2026-05-05)

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

Version	Source	Type	Score	Severity	Vector
4.0	cve_disclosure@tech.gov.sg	Secondary	2.9	LOW	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:L/SI:L/SA
4.0	CNA	CVSS	2.9	LOW	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:L/SI:L/SA

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

Low

Integrity

Low

Availability

Low

Sub Conf.

Low

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:L/SI:L/SA:N/E:P/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:N/AU:N/R:U/V:D/RE:L/U:Green

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Visualfc	Liteide	affected x38.4 git	Not specified

References

Reference	Source	Link	Tags
github.com/visualfc/liteide/pull/1325	cve_disclosure@tech.gov.sg	github.com	
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: TITAN Team (titancaproject@gmail.com) (en)

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

CVE.report and Source URL Uptime Status status.cve.report