NGINX ngx_http_proxy_v2_module vulnerability

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

Summary

CVE	CVE-2026-42926
State	PUBLISHED
Assigner	f5
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-13 16:16:49 UTC
Updated	2026-05-13 16:27:11 UTC
Description	When NGINX Open Source is configured to proxy HTTP/2 traffic by setting proxy_http_version to 2, and also uses proxy_s

Risk And Classification

Primary CVSS: v4.0 6.3 MEDIUM from f5sirt@f5.com

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:L/SA:N/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-172 | CWE-172 CWE-172 Encoding Error

Version	Source	Type	Score	Severity	Vector
4.0	f5sirt@f5.com	Secondary	6.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:L/SA:N/E:X/C...
4.0	CNA	CVSS	6.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:L/SA:N
3.1	f5sirt@f5.com	Primary	5.8	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N
3.1	CNA	CVSS	5.8	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

None

Confidentiality

None

None

Integrity

None

Availability

None

Sub Conf.

None

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:L/SA:N/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

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

None

Integrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	F5	NGINX Open Source	unaffected 1.31.0 * semver	Not specified
CNA	F5	NGINX Open Source	affected 1.29.4 1.30.1 semver	Not specified

References

Reference	Source	Link	Tags
my.f5.com/manage/s/article/K000161131	f5sirt@f5.com	my.f5.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: F5 acknowledges Mufeed VH of Winfunc Research and Hcamael of aipyaipy for bringing this issue to our attention and following the highest standards of coordinated disclosure. (en)

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