



Inadequate access control vulnerability in Fullstep

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

Summary

CVE	CVE-2026-5749
State	PUBLISHED
Assigner	INCIBE
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-22 14:17:05 UTC
Updated	2026-04-22 21:23:52 UTC
Description	Inadequate access control in the registration process in Fullstep V5, which could allow unauthenticated users to obtain a va

Risk And Classification

Primary CVSS: v4.0 8.7 HIGH from cve-coordination@incibe.es

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-306 | CWE-306 CWE-306 Missing authentication for critical function

Version	Source	Type	Score	Severity	Vector
4.0	cve-coordination@incibe.es	Secondary	8.7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/S/
4.0	CNA	CVSS	8.7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/S/

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

None

None

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/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/MSX/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	Fullstep	Fullstep	affected 5	Not specified
CNA	Fullstep	Fullstep	unaffected 5.30.07	Not specified

References

Reference	Source	Link	Tags
www.incibe.es/en/incibe-cert/notices/aviso/multiple-vulnerabilities-fullstep	cve-coordination@incibe.es	www.incibe.es	
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: Alejandro Rivera León (en)

Additional Advisory Data

Solutions

CNA: The vulnerability has been fixed by the Fullstep team in version 5.30.07, which has been available in production since January 29, 2026.

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

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