Insecure direct object reference (IDOR) vulnerability in Fullstep

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

Summary

CVE	CVE-2026-5750
State	PUBLISHED
Assigner	INCIBE
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-22 14:17:06 UTC
Updated	2026-04-22 21:23:52 UTC
Description	An insecure direct object reference (IDOR) vulnerability in the Fullstep V5 registration process allows authenticated users to

Risk And Classification

Primary CVSS: v4.0 7.6 HIGH from cve-coordination@incibe.es

CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:H/VI:H/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/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-639 | CWE-639 CWE-639 Authorization bypass through User-Controlled key

Version	Source	Type	Score	Severity	Vector
4.0	cve-coordination@incibe.es	Secondary	7.6	HIGH	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA
4.0	CNA	CVSS	7.6	HIGH	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

Low

User Interaction

None

Confidentiality

High

Integrity

High

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:H/VI:H/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/MSC:X/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.