Saleor has Cross-Account Email Change via Unbound Confirmation Token

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

Summary

CVE	CVE-2026-35407
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-08 19:25:24 UTC
Updated	2026-04-08 21:26:13 UTC
Description	Saleor is an e-commerce platform. From 2.10.0 to before 3.23.0a3, 3.22.47, 3.21.54, and 3.20.118, a business-logic and au

Risk And Classification

Primary CVSS: v4.0 5.9 MEDIUM from security-advisories@github.com

CVSS:4.0/AV:N/AC:H/AT:P/PR:L/UI:P/VC:N/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

EPSS: 0.000460000 probability, percentile 0.142630000 (date 2026-04-09)

Problem Types: CWE-285 | CWE-285 CWE-285: Improper Authorization

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	5.9	MEDIUM	CVSS:4.0/AV:N/AC:H/AT:P/PR:L/UI:P/VC:N/VI:H/VA:N/SC:N/S
4.0	CNA	DECLARED	5.9	MEDIUM	CVSS:4.0/AV:N/AC:H/AT:P/PR:L/UI:P/VC:N/VI:H/VA:N/SC:N/S

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

Present

Privileges Required

Low

User Interaction

Passive

Confidentiality

None

Integrity

High

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:H/AT:P/PR:L/UI:P/VC:N/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	Saleor	Saleor	affected >= 2.10.0, < 3.20.118	Not specified
CNA	Saleor	Saleor	affected >= 3.21.0-a.0, < 3.21.54	Not specified
CNA	Saleor	Saleor	affected >= 3.22.0-a.0, < 3.22.47	Not specified
CNA	Saleor	Saleor	affected >= 3.23.0-a.0, < 3.23.0a3	Not specified

References

Reference	Source	Link	Tags
github.com/saleor/saleor/commit/f0371bdd4cafcc841f1a9e7049cead6133bf7464	security-advisories@github.com	github.com	
github.com/saleor/saleor/commit/d6a94e95bd77f3f733fa66afd1b1ac72e863ca2a	security-advisories@github.com	github.com	
github.com/saleor/saleor/commit/cdb66da97abb7c86939e384914cd8d9194f378e8	security-advisories@github.com	github.com	
github.com/saleor/saleor/commit/7be352fa8c35875d6e66d36493ca7c14c101bd64	security-advisories@github.com	github.com	
github.com/saleor/saleor/commit/e42aa4d6e588982e78942b033af051c8ec8f43fa	security-advisories@github.com	github.com	
github.com/saleor/saleor/security/advisories/GHSA-hwph-9537-mc3p	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni

No vendor comments have been submitted for this CVE.

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