securØ

← Back to list

CVE-2026-13164 · High · June 24, 2026

Unauthenticated self-registration in MailerUp allows access to stored email data

S0 Secur0 CNA
CVE-2026-13164

Description

Missing Authentication for Critical Function (CWE-306) in `RegisterView` (`apps/accounts/views.py`), exposed at `POST /api/auth/register/`, in MailerUp <1.0.1 allows a remote, unauthenticated attacker to self-register a working account on instances where registration was intended to be restricted, because the endpoint applies the `AllowAny` permission with no email verification, CAPTCHA, or administrator approval. Any account created this way can read all production email stored by the instance, resulting in full disclosure of stored messages to an arbitrary unauthenticated attacker.

Weakness type (CWE)

CWE-306: Missing Authentication for Critical Function

Affected versions

MailerUp before 1.0.1 (all versions prior to 1.0.1). Default status: unaffected.

Score (CVSS 4.0)

High

`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`

Solution

Upgrade to version **1.0.1 or higher**.

Patch

Commit `99eb6d4`

Credits

Darío Rivas Quero (Secur0 security team) — *finder*
Cristian Fernández Cornejo (Secur0 security team) — *finder*
Mario Álvarez Fernández — *remediation developer*
Xoán M. Otero Jorge — *analyst*
Secur0 CNA — *coordinator*

Discovery source: Internal

Official record: CVE-2026-13164

Related advisories

Medium

`CVE-2026-13163`

Lack of input validation in Mailerup input parameter leads to Open Redirect

Medium

CVE-2026-13150

SSRF in Pentestify PDF generation endpoint via crafted Host header

Cybersecurity powered by ethical hackers.

SERVICES

Bug bounty

Pentesting

Crowdsourced pentesting

Vulnerability disclosure

COMPANIES

Companies FAQ

RESOURCES

Partners

Blog