mailcow: dockerized vulnerable to Second Order SQL Injection in quarantine category via API

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

Summary

CVE	CVE-2026-40871
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-21 20:17:00 UTC
Updated	2026-04-21 21:16:43 UTC
Description	mailcow: dockerized is an open source groupware/email suite based on docker. Versions prior to 2026-03b have a second-

Risk And Classification

Primary CVSS: v3.1 7.2 HIGH from security-advisories@github.com

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

Problem Types: CWE-20 | CWE-89 | CWE-116 | CWE-564 | CWE-20 CWE-20: Improper Input Validation | CWE-89 CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | CWE-116 CWE-116: Improper Encoding or Escaping of Output | CWE-564 CWE-564: SQL Injection: Hibernate

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

Confidentiality

High

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Mailcow	Mailcow-dockerized	affected < 2026-03b	Not specified

References

Reference	Source	Link
github.com/mailcow/mailcow-dockerized/security/advisories/GHSA-r8fq-wrfm...	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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