



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

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

## Summary

<b>CVE</b>	CVE-2026-40871
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-21 20:17:00 UTC
<b>Updated</b>	2026-04-21 21:16:43 UTC
<b>Description</b>	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	<a href="https://github.com">github.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.cve.org). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses/mitre).

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)