



mailcow: dockerized vulnerable to stored XSS in autodiscover logs email address field

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2026-40872 |
| 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 20:17:00 UTC |
| Description | mailcow: dockerized is an open source groupware/email suite based on docker. In versions prior to 2026-03b, the admin da |

Risk And Classification

Primary CVSS: v4.0 9.3 CRITICAL from security-advisories@github.com

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

Problem Types: CWE-79 | CWE-80 | CWE-79 CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | CWE-80 CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)

| Version | Source | Type | Score | Severity | Vector |
|---------|--------------------------------|-----------|-------|----------|---|
| 4.0 | security-advisories@github.com | Secondary | 9.3 | CRITICAL | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:H |
| 4.0 | CNA | DECLARED | 9.3 | CRITICAL | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:H |

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

Passive

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

High

Sub Integrity

High

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:H/SI:H/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/MSX/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 | Mailcow | Mailcow-dockerized | affected < 2026-03b | Not specified |

References

| Reference | Source | Link | Tags |
|---|--------------------------------|--------------|------------|
| github.com/mailcow/mailcow-dockerized/security/advisories/GHSA-f9xf-vc72... | security-advisories@github.com | github.com | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, |

No vendor comments have been submitted for this CVE.

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

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

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

CVE.report and Source URL Uptime Status [status.cve.report](#)