



# Admidio: Missing CSRF Protection on Registration Approval Actions

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

## Summary

<b>CVE</b>	CVE-2026-34384
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-31 21:16:30 UTC
<b>Updated</b>	2026-04-01 18:31:30 UTC
<b>Description</b>	Admidio is an open-source user management solution. Prior to version 5.0.8, the create_user, assign_member, and assign

## Risk And Classification

**Primary CVSS:** v3.1 7.3 HIGH from nvd@nist.gov

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

**EPSS:** 0.000130000 probability, percentile 0.021610000 (date 2026-04-01)

**Problem Types:** CWE-352 | CWE-352 CWE-352: Cross-Site Request Forgery (CSRF)

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N
3.1	security-advisories@github.com	Secondary	4.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:H/A:N
3.1	CNA	DECLARED	4.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:H/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

None

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Admidio	Admidio	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Admidio	Admidio	affected < 5.0.8	Not specified

### References

Reference	Source	Link
github.com/Admidio/admidio/commit/707171c188b3e8f36007fc3f2bccbfac896ed019	security-advisories@github.com	github.com
github.com/Admidio/admidio/security/advisories/GHSA-ph84-r98x-2j22	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go

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.

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