



CVE-2021-40347

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2021-40347
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-09-10 19:15:00 UTC
Updated	2021-09-24 03:04:00 UTC
Description	An issue was discovered in views/list.py in GNU Mailman Postorius before 1.3.5. An attacker (logged into any account) can

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Postorius Project	Postorius	All	All	All	All

References

Reference	
Debian -- Security Information -- DSA-4970-1 postorius	D
Tags · GNU Mailman / Postorius · GitLab	M
T289798 lists.wikimedia.org allows unsubscribing other users without prior confirmation (CVE-2021-40347)	M
Not Found	M
Check a user owns the email they are trying to unsubscribe (CVE-2021-40347) (3d880c56) · Commits · GNU Mailman / Postorius · GitLab	C
#993746 - python3-django-postorius: CVE-2021-40347 New upstream to fix security bug - Debian Bug report logs	C
CVE Program record	C
NVD vulnerability detail	N

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[178791](#) Debian Security Update for postorius (DSA 4970-1)

© [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](#)