



CVE-2022-37705

Published on: Not Yet Published

Last Modified on: 06/06/2023 06:15:00 PM UTC

CVE-2022-37705

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Amanda](#) from [Zmanda](#) contain the following vulnerability:

A privilege escalation flaw was found in Amanda 3.5.1 in which the backup user can acquire root privileges. The vulnerable component is the runtar SUID program, which is a wrapper to run /usr/bin/tar with specific arguments that are controllable by the attacker. This program mishandles the arguments passed to tar binary (it expects that the argument name and value are separated with a space; however, separating them with an equals sign is also supported),

CVE-2022-37705 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.7 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	HIGH	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
Amanda Network Backup: Open Source Backup for Linux, Windows, UNIX and OS X	www.amanda.org text/html	MISC www.amanda.org/
[SECURITY] Fedora 36 Update: amanda-3.5.3-1.fc36 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2023-1293196f34
Fixes Open Vulnerability CVE-2022-37705 by prajwaltr93 · Pull Request #196 · zmanda/amanda · GitHub	github.com text/html	MISC github.com/zmanda/amanda/pull/196
MARC: Mailing list ARCHives	marc.info text/html	MISC marc.info/?l=amanda-hackers

CVE-2022-37703 - directory existence disclosure via SUID calcsiz binary · Issue #192 · zmanda/amanda · GitHub	github.com text/html	 MISC github.com/zmanda/amanda/issues/192
Fixes Open Vulnerability CVE-2022-37705 by prajwaltr93 · Pull Request #194 · zmanda/amanda · GitHub	github.com text/html	 MISC github.com/zmanda/amanda/pull/194
[SECURITY] Fedora 37 Update: amanda-3.5.3-1.fc37 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2023-e295804b3d
[SECURITY] Fedora 38 Update: amanda-3.5.3-1.fc38 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2023-3d0619d767
GitHub - MaherAzzouzi/CVE-2022-37705: Amanda 3.5.1 second LPE.	github.com text/html	 MISC github.com/MaherAzzouzi/CVE-2022-37705
Fix to backups failing after Fix to CVE-2022-37705 runtar.c by prajwaltr93 · Pull Request #204 · zmanda/amanda · GitHub	github.com text/html	 MISC github.com/zmanda/amanda/pull/204
Release tag-community-3.5.3 · zmanda/amanda · GitHub	github.com text/html	 MISC github.com/zmanda/amanda/releases/tag/tag-community-3.5.3

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

- [184314](#) Debian Security Update for amanda (CVE-2022-37705)
- [199250](#) Ubuntu Security Notification for amanda Vulnerabilities (USN-5966-1)
- [283847](#) Fedora Security Update for amanda (FEDORA-2023-e295804b3d)
- [283848](#) Fedora Security Update for amanda (FEDORA-2023-1293196f34)
- [284223](#) Fedora Security Update for amanda (FEDORA-2023-3d0619d767)

Exploit/POC from Github

Amanda 3.5.1 second LPE.

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Zmanda	Amanda	3.5.1	All	All	All
cpe:2.3:a:zmanda:amanda:3.5.1:****:****:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @maherazz2	Those will be CVE-2022-37705 and CVE-2022-37706.	2022-10-13 18:10:15

© [CVE.report](#) 2023  |

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](#)