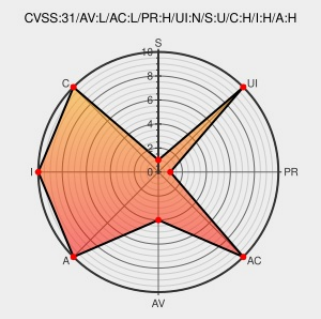
CVE-2022-37704

Published on: Not Yet Published

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

CVE-2022-37704

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Amanda from Zmanda contain the following vulnerability:

Amanda 3.5.1 allows privilege escalation from the regular user backup to root. The SUID binary located at /lib/amanda/rundump will execute /usr/sbin/dump as root with controlled arguments from the attacker which may lead to escalation of privileges, denial of service, and information disclosure.

CVE-2022-37704 has been assigned by 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/
Update the fix for CVE-2022-37704 by pcahyna · Pull Request #205 · zmanda/amanda · GitHub	github.com text/html	MISC github.com/zmanda/amanda/pull/205
[SECURITY] Fedora 36 Update: amanda-3.5.3-1.fc36 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2023-1293196f34
MARC: Mailing list ARChives	marc.info text/html	MISC marc.info/?l=amanda-hackers
CVE-2022-37703 - directory existence disclosure via SUID calcsize binary · Issue #192 · zmanda/amanda · GitHub	github.com text/html	MISC github.com/zmanda/amanda/issues/192
[SECURITY] Fedora 37 Update: amanda-3.5.3-1.fc37 - package-	lists.fedoraproject.org	FEDORA FEDORA-2023-e295804b3d

[SECURITY] Fedora 37 Update: amanda-3.5.3-1.fc37 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2023-e295804b3d
GitHub - MaherAzzouzi/CVE-2022-37704: Amanda 3.5.1 LPE	github.com text/html	MISC github.com/MaherAzzouzi/CVE-2022-37704
[SECURITY] [DLA 3330-1] amanda security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20230221 [SECURITY] [DLA 3330-1] amanda security update
[SECURITY] Fedora 38 Update: amanda-3.5.3-1.fc38 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2023-3d0619d767
CVE-2022-37704 - privilege escalation form amandabackup user to root -fix by seetharaman-rajagopal · Pull Request #197 · zmanda/amanda · GitHub	github.com text/html	MISC github.com/zmanda/amanda/pull/197
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

Related QID Numbers

181598 Debian Security Update for amanda (DLA 3330-1)

181895 Debian Security Update for amanda (CVE-2022-37704)

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 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)

← Previous ID Next ID→