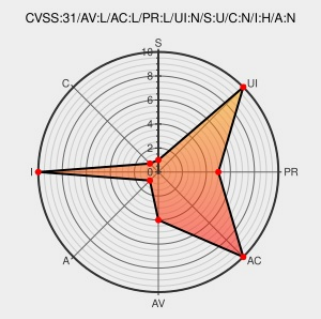
CVE-2021-27851

Published on: 04/26/2021 12:00:00 AM UTC

Last Modified on: 07/29/2022 04:34:00 PM UTC

CVE-2021-27851

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



Certain versions of Guix from Gnu contain the following vulnerability:

A security vulnerability that can lead to local privilege escalation has been found in 'guix-daemon'. It affects multi-user setups in which 'guix-daemon' runs locally. The attack consists in having an unprivileged user spawn a build process, for instance with `guix build`, that makes its build directory world-writable. The user then creates a hardlink to a root-owned file such as /etc/shadow in that build directory. If the user passed the --keep-failed option and the build eventually fails, the daemon changes ownership of the whole build tree, including the hardlink, to the user. At that point, the user has write access to the target file. Versions after and including v0.11.0-3298-g2608e40988, and versions prior to v1.2.0-75109-g94f0312546 are vulnerable.

CVE-2021-27851 has been assigned by cert@cert.org to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **GNU Guix** - **guix-daemon** version **>= v0.11.0-3298-g2608e40988**

Affected Vendor/Software: **GNU Guix** - **guix-daemon** version **< v1.2.0-75109-g94f0312546**

CVSS3 Score: 5.5 - MEDIUM

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

CVSS2 Score: 2.1 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**

NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Risk of local privilege escalation via guix-daemon — 2021 — Blog — GNU Guix	guix.gnu.org text/html	MISC guix.gnu.org/en/blog/2021/risk-of-local-privilege-escalation-via-guix-daemon/
#47229 - Local privilege escalation via guix-daemon and '--keep-failed' - GNU bug report logs	bugs.gnu.org text/html	MISC bugs.gnu.org/47229

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

179464 Debian Security Update for guix (CVE-2021-27851)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Guix	All	All	All	All

cpe:2.3:a:gnu:guix:*:*:*:*:*:*:*:*:

Discovery Credit

Nathan Nye of WhiteBeam Security

Social Mentions

Source	Title	Posted (UTC)
@oss_security	Re: Risk of local privilege escalation in GNU Guix: Posted by Leo Famulari on Apr 10This is CVE-2021-27851. We are… twitter.com/i/web/status/1…	2021-04-10 18:26:02
@CVEreport	CVE-2021-27851 : A security vulnerability that can lead to local privilege escalation has been found in 'guix-daemo… twitter.com/i/web/status/1…	2021-04-26 15:37:11

← Previous ID

Next ID→