Bug 882521 (CVE-2022-36227) - <app-arch/libarchive-3.6.1-r1: null pointer dereference

Status: RESOLVED FIXED
Alias: CVE-2022-36227
Product: Gentoo Security
Component: Vulnerabilities (show other bugs)
Hardware: All Linux
Importance: Normal normal
Assignee: Gentoo Security
URL: https://github.com/libarchive/libarch...
Whiteboard: A3 [glsa+]
Keywords: PullRequest
Depends on:
Blocks:

Reported: 2022-11-22 15:47 UTC by John Helmert III
Modified: 2023-09-29 13:40 UTC (History)
CC List: 1 user (show)
See Also: https://github.com/gentoo/gentoo/pull/28560

Attachments
Add an attachment (proposed patch, testcase, etc.)

Note
You need to log in before you can comment on or make changes to this bug.

Note: Please do not mark this bug as resolved after bumping or stabilizing. The Security Team will take care of that. Thanks.

John Helmert III AT Infra Dev Sec **2022-11-22 15:47:04 UTC** Description

```
CVE-2022-36227:

In libarchive 3.6.1, the software does not check for an error after calling calloc
function that can return with a NULL pointer if the function fails, which leads to
a resultant NULL pointer dereference or, in some cases, even arbitrary code
execution.

No idea how a null pointer dereference could lead to code
execution. Unreleased patch is:
https://github.com/libarchive/libarchive/commit/fd180c36036df7181a64931264732a10ad8cd024
```

John Helmert III AT Infra Dev Sec **2022-11-24 00:25:58 UTC** Comment 1

```
The reporter alleges this can achieve code execution on platforms where privileged
code actually reads from the 0x0 memory address. I don't know of that being the
case anywhere Gentoo is supported.
```

Michał Górny AT Infra Dev Sec **2022-12-06 04:49:59 UTC** Comment 2

The fix looks trivial-ish, so I'll just put it straight to stable.

Larry the Git Cow Dev **2022-12-06 06:02:29 UTC** Comment 3

The bug has been closed via the following commit(s):

https://gitweb.gentoo.org/repo/gentoo.git/commit/?id=b618d6ec93c66f91c071c99c65775aaef2471bdf

commit b618d6ec93c66f91c071c99c65775aaef2471bdf
Author: Meena Shanmugam <meenashanmugam@google.com>
AuthorDate: 2022-12-06 00:32:30 +0000
Commit: Michał Górny <mgorny@gentoo.org>
CommitDate: 2022-12-06 06:02:16 +0000

app-arch/libarchive: Add patch to fix CVE-2022-36227.

New version is not released in libarchive with the CVE-2022-36227 fix.

Closes: https://bugs.gentoo.org/882521
Signed-off-by: Meena Shanmugam <meenashanmugam@google.com>
Closes: https://github.com/gentoo/gentoo/pull/28560
Signed-off-by: Michał Górny <mgorny@gentoo.org>

.../files/libarchive-3.6.1-CVE-2022-36227.patch | 35 ++++++++++++++++++++++++++++++++++
...ive-3.6.1.ebuild => libarchive-3.6.1-r1.ebuild} | 2 ++
2 files changed, 37 insertions(+)

Michał Górny AT Infra Dev Sec **2022-12-06 14:26:31 UTC** Comment 4

Sorry, didn't intend to close it.

Cleaned up now, anyway.

John Helmert III AT Infra Dev Sec **2022-12-08 01:23:59 UTC** Comment 5

Thanks!

Parag **2023-02-21 07:42:45 UTC** Comment 6

Hi,
I am a beginner to CVEs vulnerability issues, So I want how to fix this issue in the Ubuntu 22.04 server.

I want to step in to fix this issue.

Parag **2023-02-21 07:45:33 UTC** Comment 7

This package info is
Package: libarchive13
Version: 3.6.0-1ubuntu1

John Helmert III AT Infra Dev Sec **2023-02-22 00:07:37 UTC** Comment 8

(In reply to Parag from comment #6)
> Hi,
> I am a beginner to CVEs vulnerability issues, So I want how to fix this
> issue in the Ubuntu 22.04 server.

>
> I want to step in to fix this issue.

Why would you ask Gentoo about Ubuntu?

John Helmert III AT Infra Dev Sec **2023-09-25 04:24:34 UTC** Comment 9

GLSA request filed.

Larry the Git Cow Dev **2023-09-29 13:39:37 UTC** Comment 10

The bug has been referenced in the following commit(s):

https://gitweb.gentoo.org/data/glsa.git/commit/?id=e05346e205e470b799ae6c0dafb506d6aa1cdae8

```
commit e05346e205e470b799ae6c0dafb506d6aa1cdae8
Author:     GLSAMaker <glsamaker@gentoo.org>
AuthorDate: 2023-09-29 13:38:51 +0000
Commit:     Hans de Graaff <graaff@gentoo.org>
CommitDate: 2023-09-29 13:39:30 +0000

    [ GLSA 202309-14 ] libarchive: Multiple Vulnerabilities

    Bug: https://bugs.gentoo.org/882521
    Bug: https://bugs.gentoo.org/911486
    Signed-off-by: GLSAMaker <glsamaker@gentoo.org>
    Signed-off-by: Hans de Graaff <graaff@gentoo.org>

 glsa-202309-14.xml | 43 ++++++++++++++++++++++++++++++++++++++++++++++++++++
 1 file changed, 43 insertions(+)
```