Bug 866237 (CVE-2021-46848) - <dev-libs/libtasn1-4.19.0: Out of bounds read

Status: RESOLVED FIXED
Alias: CVE-2021-46848
Product: Gentoo Security
Component: Vulnerabilities (show other bugs)
Hardware: All Linux
Importance: Normal minor
Assignee: Gentoo Security
URL:
Whiteboard: B3 [noglsa]
Keywords:
Depends on: ~~868138~~
Blocks:
Show dependency tree

Reported: 2022-08-24 00:19 UTC by Sam James
Modified: 2023-10-20 07:17 UTC (History)
CC List: 1 user (show)
See Also: https://gitlab.com/gnutls/libtasn1/-/issues/32

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.

Sam James AT Infra Dev Sec **2022-08-24 00:19:33 UTC** Description

```
Release notes for 4.19.0 say:
* Noteworthy changes in release 4.19.0 (2022-08-23) [stable]
- Clarify libtasn1.map license.  Closes: #38.
- Fix ETYPE_OK out of bounds read.  Closes: #32.
- Update gnulib files and various maintenance fixes.
```

Larry the Git Cow Dev **2022-08-24 00:21:33 UTC** Comment 1

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

https://gitweb.gentoo.org/repo/gentoo.git/commit/?id=8f20142212ed5c0af56b490f707e5fdff8138481

```
commit 8f20142212ed5c0af56b490f707e5fdff8138481
Author:     Sam James <sam@gentoo.org>
AuthorDate: 2022-08-24 00:18:10 +0000
Commit:     Sam James <sam@gentoo.org>
CommitDate: 2022-08-24 00:20:39 +0000
```

```
    dev-libs/libtasn1: add 4.19.0

    Licensing was also clarified upstream:
https://gitlab.com/gnutls/libtasn1/-/issues/38.

    Bug: https://gitlab.com/gnutls/libtasn1/-/issues/38
    Bug: https://bugs.gentoo.org/866237
    Signed-off-by: Sam James <sam@gentoo.org>

 dev-libs/libtasn1/Manifest               |  2 ++
 dev-libs/libtasn1/libtasn1-4.19.0.ebuild | 55 ++++++++++++++++++++++++++++++++++
 2 files changed, 57 insertions(+)
```

Larry the Git Cow Dev **2022-09-23 02:09:23 UTC** Comment 2

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

https://gitweb.gentoo.org/repo/gentoo.git/commit/?id=8c4bd08fb54e718a400e503a515dbede0fd3d4d8

```
commit 8c4bd08fb54e718a400e503a515dbede0fd3d4d8
Author:     Sam James <sam@gentoo.org>
AuthorDate: 2022-09-23 02:00:24 +0000
Commit:     Sam James <sam@gentoo.org>
CommitDate: 2022-09-23 02:08:52 +0000

    dev-libs/libtasn1: drop 4.18.0

    Bug: https://bugs.gentoo.org/866237
    Signed-off-by: Sam James <sam@gentoo.org>

 dev-libs/libtasn1/Manifest               |  1 -
 dev-libs/libtasn1/libtasn1-4.18.0.ebuild | 53 ---------------------------------
 2 files changed, 54 deletions(-)
```

John Helmert III AT Infra Dev Sec **2022-10-22 02:13:57 UTC** Comment 3

OOB read in a library, very unlikely to be exploitable, no GLSA. All done!

Also, CVE requested.

Marko Kohtala **2023-10-20 05:48:30 UTC** Comment 4

The Alias CVE appears to be wrong. Correct would be CVE-2021-46848.

Format For Printing - XML - Clone This Bug - Clone In The Same Product - Top of page