Bug 26923 (CVE-2020-29562) - Assertion failure in iconv when converting invalid UCS4 (CVE-2020-29562)

Status: RESOLVED FIXED

Alias: CVE-2020-29562

Product: glibc
Component: locale (show other bugs)
Version: 2.30

Importance: P2 normal
Target Milestone: 2.33
Assignee: Not yet assigned to anyone

URL:
Keywords:

Depends on:
Blocks:

Reported: 2020-11-19 18:22 UTC by Michael Colavita
Modified: 2022-10-07 08:20 UTC (History)
CC List: 5 users (show)

See Also:
Host:
Target:
Build:
Last reconfirmed: 2020-11-19 00:00:00

Flags: siddhesh: security+

Attachments	
An example of an iconv call that causes an assertion failure. (268 bytes, text/x-csrc) 2020-11-19 18:22 UTC, Michael Colavita	Details
Add an attachment (proposed patch, testcase, etc.)	View All

Note

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

Michael Colavita 2020-11-19 18:22:41 UTC **Description**

Created attachment 12978 [details]
An example of an iconv call that causes an assertion failure.

When converting UCS4 containing an irreversible character, an assertion failure can occur within __gconv_transform_ucs4_internal. See attachment for an easy reproducible example.

Carlos O'Donell 2020-11-19 18:40:03 UTC **Comment 1**

I can confirm this causes an assertion failure.

```
test: ../iconv/skeleton.c:746: __gconv_transform_ucs4_internal: Assertion `outbuf
== outerr' failed.
Aborted (core dumped)
```

Michael Colavita 2020-11-19 18:42:13 UTC **Comment 2**

(In reply to Carlos O'Donell from comment #1)
> I can confirm this causes an assertion failure.
>
> test: ../iconv/skeleton.c:746: __gconv_transform_ucs4_internal: Assertion
> `outbuf == outerr' failed.
> Aborted (core dumped)

I believe the root cause is due to improper bounds used when converting UCS4 to the internal UCS4-like format. I have submitted a patch that I believe should resolve the issue and explains the problem in a bit more depth.

Carlos O'Donell 2020-11-19 18:43:37 UTC **Comment 3**

Patch posted:
https://sourceware.org/pipermail/libc-alpha/2020-November/119822.html

Pádraig Brady 2020-11-19 21:06:51 UTC **Comment 4**

The fix for ~~bug 18830~~ may have been the trigger.

Siddhesh Poyarekar 2020-12-07 17:19:39 UTC **Comment 5**

Fixed in master.

```
commit 228edd356f03bf62dcf2b1335f25d43c602ee68d
Author: Michael Colavita <mcolavita@fb.com>
Date:   Thu Nov 19 11:44:40 2020 -0500

    iconv: Fix incorrect UCS4 inner loop bounds (BZ#26923)

    Previously, in UCS4 conversion routines we limit the number of
    characters we examine to the minimum of the number of characters in the
    input and the number of characters in the output. This is not the
    correct behavior when __GCONV_IGNORE_ERRORS is set, as we do not consume
    an output character when we skip a code unit. Instead, track the input
    and output pointers and terminate the loop when either reaches its
    limit.

    This resolves assertion failures when resetting the input buffer in a step of
    iconv, which assumes that the input will be fully consumed given sufficient
    output space.
```

cvs-commit@gcc.gnu.org 2020-12-08 14:35:15 UTC **Comment 6**

The master branch has been updated by Siddhesh Poyarekar <siddhesh@sourceware.org>:

https://sourceware.org/git/gitweb.cgi?p=glibc.git;h=38a9e93cb1c58e3c899d638480e6d6e42af8e6fc

```
commit 38a9e93cb1c58e3c899d638480e6d6e42af8e6fc
Author: Siddhesh Poyarekar <siddhesh@sourceware.org>
Date:   Mon Dec 7 22:29:18 2020 +0530

    Add NEWS entry for CVE-2020-29562 (BZ #26923)

    BZ #26923 now has a CVE entry, so add a NEWS entry for it.
```

cvs-commit@gcc.gnu.org 2021-01-03 13:47:46 UTC **Comment 7**

The release/2.31/master branch has been updated by Aurelien Jarno <aurel32@sourceware.org>:

https://sourceware.org/git/gitweb.cgi?p=glibc.git;h=0858f46440db4936303de0117908c1de7f4f8215

```
commit 0858f46440db4936303de0117908c1de7f4f8215
```

```
Author: Siddhesh Poyarekar <siddhesh@sourceware.org>
Date:   Mon Dec 7 22:29:18 2020 +0530

    Add NEWS entry for CVE-2020-29562 (BZ #26923)

    BZ #26923 now has a CVE entry, so add a NEWS entry for it.

    (cherry picked from commit 38a9e93cb1c58e3c899d638480e6d6e42af8e6fc)
```

cvs-commit@gcc.gnu.org 2021-09-21 00:54:43 UTC **Comment 8**

The release/2.27/master branch has been updated by Dmitry Levin
<ldv@sourceware.org>:

https://sourceware.org/git/gitweb.cgi?p=glibc.git;h=3668134a9ef34b1a96f6b56666ae04886a99d33f

```
commit 3668134a9ef34b1a96f6b56666ae04886a99d33f
Author: Siddhesh Poyarekar <siddhesh@sourceware.org>
Date:   Mon Dec 7 22:29:18 2020 +0530

    Add NEWS entry for CVE-2020-29562 (BZ #26923)

    BZ #26923 now has a CVE entry, so add a NEWS entry for it.

    (cherry picked from commit 38a9e93cb1c58e3c899d638480e6d6e42af8e6fc)
```

cvs-commit@gcc.gnu.org 2022-10-07 08:20:34 UTC **Comment 9**

The release/2.32/master branch has been updated by Dmitry Levin
<ldv@sourceware.org>:

https://sourceware.org/git/gitweb.cgi?p=glibc.git;h=6fd634e9b922a4a1293f0cf5a8f6c908f68c5401

```
commit 6fd634e9b922a4a1293f0cf5a8f6c908f68c5401
Author: Siddhesh Poyarekar <siddhesh@sourceware.org>
Date:   Mon Dec 7 22:29:18 2020 +0530

    NEWS: Mention CVE-2020-29562 (BZ #26923)

    BZ #26923 now has a CVE entry, so add a NEWS entry for it.

    (cherry picked from commit 38a9e93cb1c58e3c899d638480e6d6e42af8e6fc)
```

Format For Printing - XML - Clone This Bug - Top of page