Bug 29289 - display_debug_names: Assertion `name_count == buckets_filled + hash_clash_count' failed

Status:	RESOLVED FIXED	**Reported:**	2022-06-26 20:35 UTC by Hex Rabbit
Alias:	None	**Modified:**	2022-06-27 12:44 UTC (History)
		CC List:	2 users (show)
Product:	binutils		
Component:	binutils (show other bugs)	**See Also:**	
		Host:	
Version:	2.39	**Target:**	
		Build:	
Importance:	P2 normal	**Last reconfirmed:**	2022-06-27 00:00:00
Target Milestone:	---		
Assignee:	Nick Clifton		
URL:			
Keywords:			
Depends on:			
Blocks:			

Attachments	
the file caused assertion failed (455 bytes, model/x.stl-binary) 2022-06-26 20:35 UTC, Hex Rabbit	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.

Hex Rabbit 2022-06-26 20:35:07 UTC Description

Created attachment 14176 [details]
the file caused assertion failed

During fuzzing campaign, I found some files triggered the assertion inside `binutils/dwarf.c:display_debug_names` with the command:

```
readelf -w file
```

Command output:

```
readelf: Warning: The e_shentsize field in the ELF header is larger than the size
of an ELF section header
readelf: Warning: Section 6 has an out of range sh_link value of 2162688
readelf: Warning: Section 7 has an out of range sh_link value of 1111638594
readelf: Warning: Section 8 has an out of range sh_link value of 14592
readelf: Warning: Section 10 has an out of range sh_link value of 237568
readelf: Warning: Section 11 has an out of range sh_link value of 4244635647
readelf: Warning: Section 12 has an out of range sh_link value of 457375744
readelf: Warning: Section 14 has an out of range sh_link value of 4278190080
```

~~~~
readelf: Warning: The e_phentsize field in the ELF header is larger than the size
of an ELF program header
readelf: Error: Reading 728 bytes extends past end of file for program headers
section '.debug_names' has the NOBITS type - its contents are unreliable.
Contents of the .debug_names section:

readelf: Warning: Debug info is corrupted, .debug_names header at 0 has length
4c457f
readelf: Error: Reading 8192 bytes extends past end of file for .debug_names
section data
Contents of the .debug_names section:

Version 5
readelf: Warning: Padding field of .debug_names must be 0 (found 0x70)
readelf: Warning: Compilation unit count must be >= 1 in .debug_names
Augmentation string:  ("")
CU table:

TU table:

Foreign TU table:

Used 1 of 1 bucket.
Out of 0 items there are 0 bucket clashes (longest of 0 entries).
readelf: ../../binutils/dwarf.c:10239: display_debug_names: Assertion `name_count
== buckets_filled + hash_clash_count' failed.
[1]    552315 abort      ./readelf -w
```
~~~~

build on latest commit (9544899f2809833729159b0acb414ef7730650d5), with default config `../configure`

cvs-commit@gcc.gnu.org 2022-06-27 12:43:53 UTC **Comment 1**

The master branch has been updated by Nick Clifton <nickc@sourceware.org>:

https://sourceware.org/git/gitweb.cgi?p=binutils-gdb.git;h=e3e5ae049371a27fd1737aba946fe26d06e029b5

```
commit e3e5ae049371a27fd1737aba946fe26d06e029b5
Author: Nick Clifton <nickc@redhat.com>
Date:   Mon Jun 27 13:43:02 2022 +0100

    Replace a run-time assertion failure with a warning message when parsing
corrupt DWARF data.
```

            ~~PR 29289~~
            * dwarf.c (display_debug_names): Replace assert with a warning message.

Nick Clifton 2022-06-27 12:44:14 UTC **Comment 2**

Resolved

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