Bug 16397 - Buildbot crash output: fuzz-2020-02-16-11740.pcap

Status: RESOLVED FIXED

Alias: None

Product: Wireshark
Component: Dissection engine (libwireshark) (show other bugs)
Version: unspecified
Hardware: x86-64 Ubuntu

Importance: High Major (vote)
Target Milestone: ---
Assignee: Bugzilla Administrator

URL:

Depends on:
Blocks:

Reported: 2020-02-17 02:40 UTC by Buildbot Builder
Modified: 2020-02-27 22:15 UTC (History)
CC List: 0 users

See Also: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9428

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.

Buildbot Builder 2020-02-17 02:40:03 UTC **Description**

```
Problems have been found with the following capture file:

https://www.wireshark.org/download/automated/captures/fuzz-2020-02-16-11740.pcap

stderr:
Input file: /home/wireshark/menagerie/menagerie/16589-
PR_1382261__pcap_for_Wireshark.snoop

Build host information:
Linux build6 4.15.0-76-generic #86-Ubuntu SMP Fri Jan 17 17:24:28 UTC 2020 x86_64
x86_64 x86_64 GNU/Linux
Distributor ID: Ubuntu
Description:    Ubuntu 18.04.4 LTS
Release:        18.04
Codename:       bionic

Buildbot information:
BUILDBOT_WORKERNAME=fuzz-test
BUILDBOT_BUILDNUMBER=391
BUILDBOT_BUILDERNAME=Fuzz Test
BUILDBOT_URL=http://buildbot.wireshark.org/wireshark-2.6/
BUILDBOT_REPOSITORY=ssh://wireshark-buildbot@code.wireshark.org:29418/wireshark
BUILDBOT_GOT_REVISION=3e8163790d0072f58957749d900986a22b8db5bc

Return value:  0

Dissector bug:  0

Valgrind error count:  6



Git commit
commit 3e8163790d0072f58957749d900986a22b8db5bc
Author: Gerald Combs <gerald@wireshark.org>
Date:   Sun Feb 16 08:58:54 2020 +0000

    [Automatic update for 2020-02-16]

    Update manuf, services enterprise numbers, translations, and other items.

    Change-Id: I2feb9bb26444e5047db077addad9b05c35582ebb
    Reviewed-on: https://code.wireshark.org/review/36119
    Reviewed-by: Gerald Combs <gerald@wireshark.org>


Command and args: ./tools/valgrind-wireshark.sh -b
/home/wireshark/builders/wireshark-2.6-fuzz/fuzztest/install/bin

==30613== Memcheck, a memory error detector
==30613== Copyright (C) 2002-2017, and GNU GPL'd, by Julian Seward et al.
==30613== Using Valgrind-3.13.0 and LibVEX; rerun with -h for copyright info
==30613== Command: /home/wireshark/builders/wireshark-2.6-
fuzz/fuzztest/install/bin/tshark -nr /fuzz/buildbot/fuzztest/valgrind-fuzz-
2.6/fuzz-2020-02-16-11740.pcap
==30613==
==30613== Invalid read of size 1
==30613==    at 0xB87F6F0: __rawmemchr_avx2 (memchr-avx2.S:46)
==30613==    by 0xB785351: _IO_str_init_static_internal (strops.c:41)
==30613==    by 0xB77160C: __isoc99_vsscanf (isoc99_vsscanf.c:41)
==30613==    by 0xB771573: __isoc99_sscanf (isoc99_sscanf.c:31)
==30613==    by 0x6DB4B2E: dissect_eap_identity_wlan (packet-eap.c:597)
==30613==    by 0x6DB60AD: dissect_eap_identity (packet-eap.c:628)
==30613==    by 0x6DB60AD: dissect_eap (packet-eap.c:910)
==30613==    by 0x6AD4D27: call_dissector_through_handle (packet.c:702)
==30613==    by 0x6AD5D44: call_dissector_work (packet.c:795)
==30613==    by 0x6AD7AA1: call_dissector_with_data (packet.c:3139)
==30613==    by 0x71FC44E: dissect_attribute_value_pairs (packet-radius.c:1832)
==30613==    by 0x71FD42B: dissect_radius (packet-radius.c:2262)
==30613==    by 0x6AD4D27: call_dissector_through_handle (packet.c:702)
==30613==  Address 0x12e606d3 is 1 bytes after a block of size 2 alloc'd
==30613==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-
linux.so)
==30613==    by 0xAA14AB8: g_malloc (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==30613==    by 0xAA2E4B9: g_strndup (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==30613==    by 0xAA2FCFD: g_strsplit_set (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==30613==    by 0x6DB49F7: dissect_eap_identity_wlan (packet-eap.c:553)
==30613==    by 0x6DB60AD: dissect_eap_identity (packet-eap.c:628)
==30613==    by 0x6DB60AD: dissect_eap (packet-eap.c:910)
==30613==    by 0x6AD4D27: call_dissector_through_handle (packet.c:702)
==30613==    by 0x6AD5D44: call_dissector_work (packet.c:795)
==30613==    by 0x6AD7AA1: call_dissector_with_data (packet.c:3139)
==30613==    by 0x71FC44E: dissect_attribute_value_pairs (packet-radius.c:1832)
==30613==    by 0x71FD42B: dissect_radius (packet-radius.c:2262)
==30613==    by 0x6AD4D27: call_dissector_through_handle (packet.c:702)
==30613==
==30613== Invalid read of size 1
==30613==    at 0x4C37064: rawmemchr (in /usr/lib/valgrind/vgpreload_memcheck-
amd64-linux.so)
==30613==    by 0xB785351: _IO_str_init_static_internal (strops.c:41)
==30613==    by 0xB77160C: __isoc99_vsscanf (isoc99_vsscanf.c:41)
==30613==    by 0xB771573: __isoc99_sscanf (isoc99_sscanf.c:31)
==30613==    by 0x6DB4B2E: dissect_eap_identity_wlan (packet-eap.c:597)
==30613==    by 0x6DB60AD: dissect_eap_identity (packet-eap.c:628)
```

```
==30613==    by 0x6DB60AD: dissect_eap (packet-eap.c:910)
==30613==    by 0x6AD4D27: call_dissector_through_handle (packet.c:702)
==30613==    by 0x6AD5D44: call_dissector_work (packet.c:795)
==30613==    by 0x6AD7AA1: call_dissector_with_data (packet.c:3139)
==30613==    by 0x71FC44E: dissect_attribute_value_pairs (packet-radius.c:1832)
==30613==    by 0x71FD42B: dissect_radius (packet-radius.c:2262)
==30613==    by 0x6AD4D27: call_dissector_through_handle (packet.c:702)
==30613==  Address 0x12e606d4 is 2 bytes after a block of size 2 alloc'd
==30613==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-
linux.so)
==30613==    by 0xAA14AB8: g_malloc (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==30613==    by 0xAA2E4B9: g_strndup (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==30613==    by 0xAA2FCFD: g_strsplit_set (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==30613==    by 0x6DB49F7: dissect_eap_identity_wlan (packet-eap.c:553)
==30613==    by 0x6DB60AD: dissect_eap_identity (packet-eap.c:628)
==30613==    by 0x6DB60AD: dissect_eap (packet-eap.c:910)
==30613==    by 0x6AD4D27: call_dissector_through_handle (packet.c:702)
==30613==    by 0x6AD5D44: call_dissector_work (packet.c:795)
==30613==    by 0x6AD7AA1: call_dissector_with_data (packet.c:3139)
==30613==    by 0x71FC44E: dissect_attribute_value_pairs (packet-radius.c:1832)
==30613==    by 0x71FD42B: dissect_radius (packet-radius.c:2262)
==30613==    by 0x6AD4D27: call_dissector_through_handle (packet.c:702)
==30613==
==30613== Invalid read of size 1
==30613==    at 0xB76075E: _IO_vfscanf (vfscanf.c:630)
==30613==    by 0xB771621: __isoc99_vsscanf (isoc99_vsscanf.c:43)
==30613==    by 0xB771573: __isoc99_sscanf (isoc99_sscanf.c:31)
==30613==    by 0x6DB4B2E: dissect_eap_identity_wlan (packet-eap.c:597)
==30613==    by 0x6DB60AD: dissect_eap_identity (packet-eap.c:628)
==30613==    by 0x6DB60AD: dissect_eap (packet-eap.c:910)
==30613==    by 0x6AD4D27: call_dissector_through_handle (packet.c:702)
==30613==    by 0x6AD5D44: call_dissector_work (packet.c:795)
==30613==    by 0x6AD7AA1: call_dissector_with_data (packet.c:3139)
==30613==    by 0x71FC44E: dissect_attribute_value_pairs (packet-radius.c:1832)
==30613==    by 0x71FD42B: dissect_radius (packet-radius.c:2262)
==30613==    by 0x6AD4D27: call_dissector_through_handle (packet.c:702)
==30613==    by 0x6AD5D44: call_dissector_work (packet.c:795)
==30613==  Address 0x12e606d3 is 1 bytes after a block of size 2 alloc'd
==30613==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-
linux.so)
==30613==    by 0xAA14AB8: g_malloc (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==30613==    by 0xAA2E4B9: g_strndup (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==30613==    by 0xAA2FCFD: g_strsplit_set (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==30613==    by 0x6DB49F7: dissect_eap_identity_wlan (packet-eap.c:553)
==30613==    by 0x6DB60AD: dissect_eap_identity (packet-eap.c:628)
==30613==    by 0x6DB60AD: dissect_eap (packet-eap.c:910)
==30613==    by 0x6AD4D27: call_dissector_through_handle (packet.c:702)
==30613==    by 0x6AD5D44: call_dissector_work (packet.c:795)
==30613==    by 0x6AD7AA1: call_dissector_with_data (packet.c:3139)
==30613==    by 0x71FC44E: dissect_attribute_value_pairs (packet-radius.c:1832)
==30613==    by 0x71FD42B: dissect_radius (packet-radius.c:2262)
==30613==    by 0x6AD4D27: call_dissector_through_handle (packet.c:702)
==30613==
==30613== Invalid read of size 1
==30613==    at 0xB783FB3: _IO_sputbackc (genops.c:666)
==30613==    by 0xB7607EB: _IO_vfscanf (vfscanf.c:635)
==30613==    by 0xB771621: __isoc99_vsscanf (isoc99_vsscanf.c:43)
==30613==    by 0xB771573: __isoc99_sscanf (isoc99_sscanf.c:31)
==30613==    by 0x6DB4B2E: dissect_eap_identity_wlan (packet-eap.c:597)
==30613==    by 0x6DB60AD: dissect_eap_identity (packet-eap.c:628)
==30613==    by 0x6DB60AD: dissect_eap (packet-eap.c:910)
==30613==    by 0x6AD4D27: call_dissector_through_handle (packet.c:702)
==30613==    by 0x6AD5D44: call_dissector_work (packet.c:795)
==30613==    by 0x6AD7AA1: call_dissector_with_data (packet.c:3139)
==30613==    by 0x71FC44E: dissect_attribute_value_pairs (packet-radius.c:1832)
==30613==    by 0x71FD42B: dissect_radius (packet-radius.c:2262)
==30613==    by 0x6AD4D27: call_dissector_through_handle (packet.c:702)
==30613==  Address 0x12e606d3 is 1 bytes after a block of size 2 alloc'd
==30613==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-
linux.so)
==30613==    by 0xAA14AB8: g_malloc (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==30613==    by 0xAA2E4B9: g_strndup (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==30613==    by 0xAA2FCFD: g_strsplit_set (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==30613==    by 0x6DB49F7: dissect_eap_identity_wlan (packet-eap.c:553)
==30613==    by 0x6DB60AD: dissect_eap_identity (packet-eap.c:628)
==30613==    by 0x6DB60AD: dissect_eap (packet-eap.c:910)
==30613==    by 0x6AD4D27: call_dissector_through_handle (packet.c:702)
==30613==    by 0x6AD5D44: call_dissector_work (packet.c:795)
==30613==    by 0x6AD7AA1: call_dissector_with_data (packet.c:3139)
==30613==    by 0x71FC44E: dissect_attribute_value_pairs (packet-radius.c:1832)
==30613==    by 0x71FD42B: dissect_radius (packet-radius.c:2262)
==30613==    by 0x6AD4D27: call_dissector_through_handle (packet.c:702)
==30613==
==30613== Invalid read of size 1
==30613==    at 0xB7610F1: _IO_vfscanf (vfscanf.c:1400)
==30613==    by 0xB771621: __isoc99_vsscanf (isoc99_vsscanf.c:43)
==30613==    by 0xB771573: __isoc99_sscanf (isoc99_sscanf.c:31)
==30613==    by 0x6DB4B2E: dissect_eap_identity_wlan (packet-eap.c:597)
==30613==    by 0x6DB60AD: dissect_eap_identity (packet-eap.c:628)
==30613==    by 0x6DB60AD: dissect_eap (packet-eap.c:910)
==30613==    by 0x6AD4D27: call_dissector_through_handle (packet.c:702)
==30613==    by 0x6AD5D44: call_dissector_work (packet.c:795)
==30613==    by 0x6AD7AA1: call_dissector_with_data (packet.c:3139)
==30613==    by 0x71FC44E: dissect_attribute_value_pairs (packet-radius.c:1832)
==30613==    by 0x71FD42B: dissect_radius (packet-radius.c:2262)
==30613==    by 0x6AD4D27: call_dissector_through_handle (packet.c:702)
==30613==    by 0x6AD5D44: call_dissector_work (packet.c:795)
==30613==  Address 0x12e606d3 is 1 bytes after a block of size 2 alloc'd
==30613==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-
linux.so)
==30613==    by 0xAA14AB8: g_malloc (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==30613==    by 0xAA2E4B9: g_strndup (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==30613==    by 0xAA2FCFD: g_strsplit_set (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==30613==    by 0x6DB49F7: dissect_eap_identity_wlan (packet-eap.c:553)
==30613==    by 0x6DB60AD: dissect_eap_identity (packet-eap.c:628)
==30613==    by 0x6DB60AD: dissect_eap (packet-eap.c:910)
==30613==    by 0x6AD4D27: call_dissector_through_handle (packet.c:702)
==30613==    by 0x6AD5D44: call_dissector_work (packet.c:795)
==30613==    by 0x6AD7AA1: call_dissector_with_data (packet.c:3139)
==30613==    by 0x71FC44E: dissect_attribute_value_pairs (packet-radius.c:1832)
==30613==    by 0x71FD42B: dissect_radius (packet-radius.c:2262)
==30613==    by 0x6AD4D27: call_dissector_through_handle (packet.c:702)
==30613==
==30613== Invalid read of size 1
==30613==    at 0xB783FB3: _IO_sputbackc (genops.c:666)
==30613==    by 0xB762C1C: _IO_vfscanf (vfscanf.c:1835)
==30613==    by 0xB771621: __isoc99_vsscanf (isoc99_vsscanf.c:43)
==30613==    by 0xB771573: __isoc99_sscanf (isoc99_sscanf.c:31)
==30613==    by 0x6DB4B2E: dissect_eap_identity_wlan (packet-eap.c:597)
==30613==    by 0x6DB60AD: dissect_eap_identity (packet-eap.c:628)
==30613==    by 0x6DB60AD: dissect_eap (packet-eap.c:910)
==30613==    by 0x6AD4D27: call_dissector_through_handle (packet.c:702)
==30613==    by 0x6AD5D44: call_dissector_work (packet.c:795)
==30613==    by 0x6AD7AA1: call_dissector_with_data (packet.c:3139)
==30613==    by 0x71FC44E: dissect_attribute_value_pairs (packet-radius.c:1832)
==30613==    by 0x71FD42B: dissect_radius (packet-radius.c:2262)
==30613==    by 0x6AD4D27: call_dissector_through_handle (packet.c:702)
==30613==  Address 0x12e606d3 is 1 bytes after a block of size 2 alloc'd
```

```
==30613==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-
linux.so)
==30613==    by 0xAA14AB8: g_malloc (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==30613==    by 0xAA2E4B9: g_strndup (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==30613==    by 0xAA2FCFD: g_strsplit_set (in /usr/lib/x86_64-linux-gnu/libglib-
2.0.so.0.5600.4)
==30613==    by 0x6DB49F7: dissect_eap_identity_wlan (packet-eap.c:553)
==30613==    by 0x6DB60AD: dissect_eap_identity (packet-eap.c:628)
==30613==    by 0x6DB60AD: dissect_eap (packet-eap.c:910)
==30613==    by 0x6AD4D27: call_dissector_through_handle (packet.c:702)
==30613==    by 0x6AD5D44: call_dissector_work (packet.c:795)
==30613==    by 0x6AD7AA1: call_dissector_with_data (packet.c:3139)
==30613==    by 0x71FC44E: dissect_attribute_value_pairs (packet-radius.c:1832)
==30613==    by 0x71FD42B: dissect_radius (packet-radius.c:2262)
==30613==    by 0x6AD4D27: call_dissector_through_handle (packet.c:702)
==30613==
==30613==
==30613== HEAP SUMMARY:
==30613==     in use at exit: 36,257 bytes in 230 blocks
==30613==   total heap usage: 444,191 allocs, 443,961 frees, 50,253,164 bytes
allocated
==30613==
==30613== LEAK SUMMARY:
==30613==    definitely lost: 520 bytes in 25 blocks
==30613==    indirectly lost: 970 bytes in 65 blocks
==30613==      possibly lost: 0 bytes in 0 blocks
==30613==    still reachable: 31,824 bytes in 118 blocks
==30613==         suppressed: 2,943 bytes in 22 blocks
==30613== Rerun with --leak-check=full to see details of leaked memory
==30613==
==30613== For counts of detected and suppressed errors, rerun with: -v
==30613== ERROR SUMMARY: 6 errors from 6 contexts (suppressed: 0 from 0)

[ no debug trace ]
```

Gerrit Code Review 2020-02-21 18:22:57 UTC Comment 1

Change 36146 had a related patch set uploaded by Gerald Combs:
EAP: Remove a couple of string length assumptions.

https://code.wireshark.org/review/36146

Gerrit Code Review 2020-02-24 07:42:41 UTC Comment 2

Change 36146 merged by Anders Broman:
EAP: Remove a couple of string length assumptions.

https://code.wireshark.org/review/36146

Gerrit Code Review 2020-02-24 14:51:42 UTC Comment 3

Change 36171 had a related patch set uploaded by Gerald Combs:
EAP: Remove a couple of string length assumptions.

https://code.wireshark.org/review/36171

Gerrit Code Review 2020-02-24 14:52:00 UTC Comment 4

Change 36172 had a related patch set uploaded by Gerald Combs:
EAP: Remove a couple of string length assumptions.

https://code.wireshark.org/review/36172

Gerrit Code Review 2020-02-24 14:52:28 UTC Comment 5

Change 36173 had a related patch set uploaded by Gerald Combs:
EAP: Remove a couple of string length assumptions.

https://code.wireshark.org/review/36173

Gerrit Code Review 2020-02-24 14:52:58 UTC Comment 6

Change 36171 merged by Gerald Combs:
EAP: Remove a couple of string length assumptions.

https://code.wireshark.org/review/36171

Gerrit Code Review 2020-02-24 14:53:11 UTC Comment 7

Change 36172 merged by Gerald Combs:
EAP: Remove a couple of string length assumptions.

https://code.wireshark.org/review/36172

Gerrit Code Review 2020-02-24 14:53:26 UTC Comment 8

Change 36173 merged by Gerald Combs:
EAP: Remove a couple of string length assumptions.

https://code.wireshark.org/review/36173

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