Closed · Issue created 2 years ago by **Jim Borden**

BLIP: Static decompression buffer is of insufficient size

Summary

Currently the BLIP dissector uses a statically allocated buffer of 16 Kb in order to store the results of decompressing a compressed message body. However, the 16 Kb figure is the maximum size of a *compressed* message frame, not an uncompressed one, so any body that has an uncompressed message larger than 16Kb will crash wireshark

Steps to reproduce

The easiest thing to do is to open the attached capture file

What is the current bug behavior?

Wireshark crashes

What is the expected correct behavior?

Wireshark correctly displays the > 16Kb decompressed body

Sample capture file

badtrace.pcapng.gz

Relevant logs and/or screenshots

No relevant logs, the crash is very straightforward

Build information

Version 3.2.6 (v3.2.6-0-g4f9257fb)

To upload designs, you'll need to enable LFS and have an admin enable hashed storage. More information

Tasks 0

No tasks are currently assigned. Use tasks to break down this issue into smaller parts.

Linked items 0

Link issues together to show that they're related or that one is blocking others. Learn more.

Related merge requests 1

BLIP: Fix decompression buffer bug

!381

When this merge request is accepted, this issue will be closed automatically.

Activity

Jim Borden mentioned in merge request !381 (merged) 2 years ago

A Wireshark GitLab Utility closed via merge request !381 (merged) 2 years ago

Gerald Combs @geraldcombs · 2 years ago — Owner

I can duplicate this here in master, master-3.2, and master-3.0 with ASAN + `tshark -nVr cbl1291.pcapng.gz`

Jim Borden @borrrden · 2 years ago — Author, Contributor

I see that you've very kindly cherry picked this into the corresponding branches for me, but out of curiosity am I supposed to be doing that as well? Or is that a task on the wireshark side?

Gerald Combs @geraldcombs · 2 years ago — Owner

Like many other aspects of the project (and open source in general), it's mainly a matter of whoever has the time and inclination. In this particular case I'm making what will likely be the last 3.0.x release so it made sense to backport the fix.

Please register or sign in to reply

Gerald Combs @geraldcombs · 2 years ago — Owner

CVE-2020-25866

Jim Borden @borrrden · 2 years ago — Author, Contributor

FYI your https://www.wireshark.org/security/wnpa-sec-2020-13 link still contains a link back to the old bugzilla installation instead of to here.

Gerald Combs @geraldcombs · 2 years ago — Owner

Fixed. Thanks!

Please register or sign in to reply

Jim Borden mentioned in commit 594d312b 2 years ago

Jim Borden mentioned in commit f1bab46d 2 years ago

Please register or sign in to reply