Starred by 1 user

Owner:	----
CC:	da...@adalogics.com reini...@gmail.com
Status:	Verified *(Closed)*
Components:	----
Modified:	Mar 18, 2021
Type:	Bug-Security

ClusterFuzz
Stability-Memory-AddressSanitizer
Reproducible
ClusterFuzz-Verified
Engine-libfuzzer
OS-Linux
Security_Severity-High
Proj-libredwg
Reported-2021-03-05
Disclosure-2021-06-03

Issue 31724: libredwg:llvmfuzz: Heap-double-free in bit_chain_free

Reported by ClusterFuzz-External on Fri, Mar 5, 2021, 4:47 AM EST Project Member

Code

Detailed Report: https://oss-fuzz.com/testcase?key=5045674581295104

Project: libredwg
Fuzzing Engine: libFuzzer
Fuzz Target: llvmfuzz
Job Type: libfuzzer_asan_libredwg
Platform Id: linux

Crash Type: Heap-double-free
Crash Address: 0x610000004e80
Crash State:
  bit_chain_free
  dwg_encode_MTEXT
  dwg_encode_add_object

Sanitizer: address (ASAN)

Recommended Security Severity: High

Regressed: https://oss-fuzz.com/revisions?job=libfuzzer_asan_libredwg&range=202102280602:202103010630

Reproducer Testcase: https://oss-fuzz.com/download?testcase_id=5045674581295104

Issue filed automatically.

See https://google.github.io/oss-fuzz/advanced-topics/reproducing for instructions to reproduce this bug locally.
When you fix this bug, please
  * mention the fix revision(s).
  * state whether the bug was a short-lived regression or an old bug in any stable releases.
  * add any other useful information.
This information can help downstream consumers.

If you need to contact the OSS-Fuzz team with a question, concern, or any other feedback, please file an issue at https://github.com/google/oss-fuzz/issues. Comments on individual Monorail issues are not monitored.

This bug is subject to a 90 day disclosure deadline. If 90 days elapse
without an upstream patch, then the bug report will automatically
become visible to the public.

Comment 1 by sheriffbot on Fri, Mar 5, 2021, 3:02 PM EST Project Member

Labels: Disclosure-2021-06-03

Comment 2 by ClusterFuzz-External on Tue, Mar 9, 2021, 11:10 AM EST Project Member

Status: Verified (was: New)
Labels: ClusterFuzz-Verified

ClusterFuzz testcase 5045674581295104 is verified as fixed in https://oss-fuzz.com/revisions?job=libfuzzer_asan_libredwg&range=202103080604:202103090610

If this is incorrect, please file a bug on https://github.com/google/oss-fuzz/issues/new

Comment 3 by sheriffbot on Thu, Mar 18, 2021, 2:57 PM EDT Project Member

Labels: -restrict-view-commit

This bug has been fixed. It has been opened to the public.

- Your friendly Sheriffbot