New issue

Jump to bottom

# AddressSanitizer: heap-use-after-free at libpff_item_tree.c:828 #62

Closed hongxuchen opened this issue on Jun 23, 2018 · 1 comment

Assignees

Labels duplicate

**hongxuchen** commented on Jun 23, 2018

POC files:
https://github.com/ntu-sec/pocs/blob/master/libpff-4938b7a/crashes/huaf_libpff_item_tree.c%3A828_1.input.txt
https://github.com/ntu-sec/pocs/blob/master/libpff-4938b7a/crashes/huaf_libpff_item_tree.c%3A828_2.input.txt

ASan output:
https://github.com/ntu-sec/pocs/blob/master/libpff-4938b7a/crashes/huaf_libpff_item_tree.c%3A828_1.err.SIG06
https://github.com/ntu-sec/pocs/blob/master/libpff-4938b7a/crashes/huaf_libpff_item_tree.c%3A828_2.err.SIG06

**joachimmetz** self-assigned this on Jun 27, 2018

**joachimmetz** added the needs a closer look label on Jun 27, 2018

**joachimmetz** commented on Jul 13, 2018 Member

This appears to be a duplicate of #61

**joachimmetz** added duplicate and removed needs a closer look labels on Jul 13, 2018

**joachimmetz** closed this as completed on Jul 13, 2018

Assignees
joachimmetz

Labels
duplicate

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

2 participants