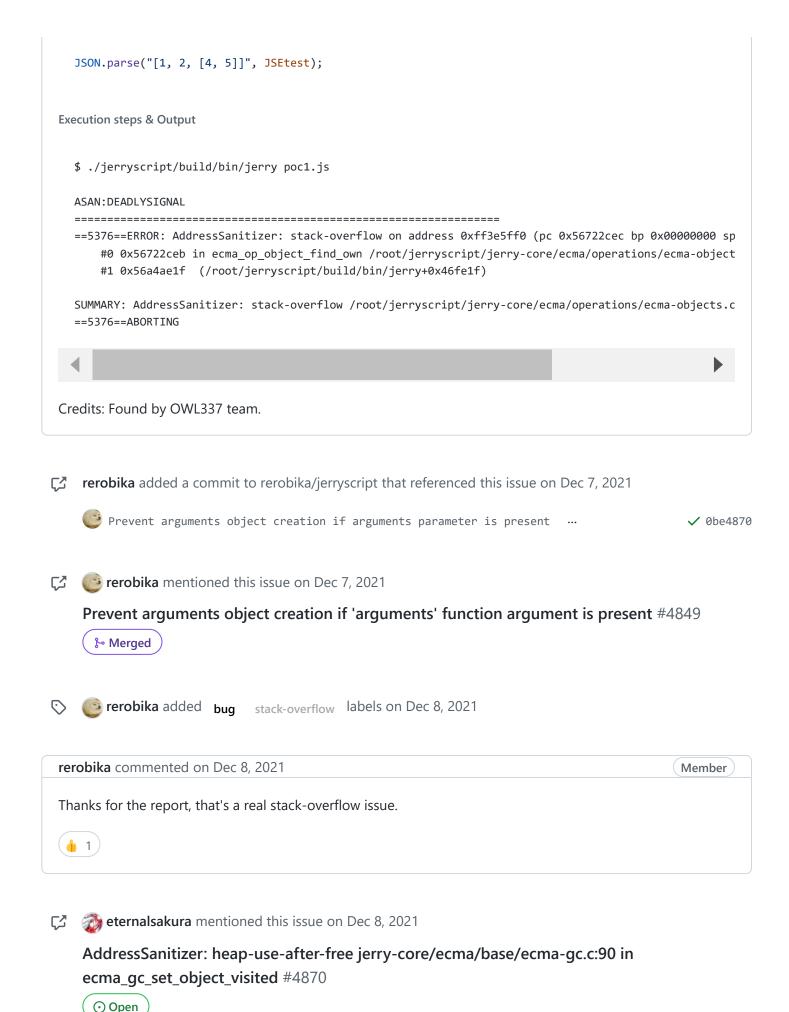
☐ jerryscript-project / jerryscript Public <> Code • Issues 71 11 Pull requests 39 Actions Wiki Security Jump to bottom New issue Stack-overflow in ecma-objects (ecma_op_object_find_own) #4848 Closed hope-fly opened this issue on Dec 7, 2021 · 1 comment · Fixed by #4877 bug stack-overflow Labels hope-fly commented on Dec 7, 2021 • edited • JerryScript revision 4592143 **Build platform** Ubuntu 18.04.5 LTS (Linux 4.19.128-microsoft-standard x86_64) Ubuntu 18.04.5 LTS (Linux 5.4.0-44-generic x86_64) **Build steps** ./tools/build.py --clean --debug --compile-flag=-fsanitize=address --compile-flag=-m32 --lto=off --lo Test case var once = false; var m = 1;function JSEtest(){ if(!once){ m = new Array(1, 2, 3);this[2] = m;once = true; return this[2] = m; }



以	rerobika added a commit to rerobika/jerryscript that referenced this issue on Dec 9, 2021	
	Prevent stackoverflow in json internalize property	✓ 33c0dfa
ÇŽ	rerobika added a commit to rerobika/jerryscript that referenced this issue on Dec 9, 2021	
	Prevent stack-overflow in json internalize property	✓ d040dc4
Ç₹	This was referenced on Dec 9, 2021	
	Prevent stack-overflow in json internalize property #4877	
	AddressSanitizer: stack-overflow in ecma_builtin_json_internalize_process_property	#4883
Ç	rerobika added a commit to rerobika/jerryscript that referenced this issue on Dec 15, 2021	
	Prevent stack-overflow in json internalize property	✓ 73ab9ee
	ssy-szeged closed this as completed in #4877 on Dec 15, 2021	
ÇŽ	ossy-szeged pushed a commit that referenced this issue on Dec 15, 2021	
	Prevent stack-overflow in json internalize property (#4877)	✓ dfc001d
Assign No one	nees e assigned	
Labels bug	stack-overflow	
Project None y		

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

Prevent stack-overflow in json internalize property rerobika/jerryscript

2 participants



