New issue

Jump to bottom

OS Command Injection in sandcat plugin #462

Closed **1c3z** opened this issue on Sep 2, 2019 · 2 comments

Labels bug

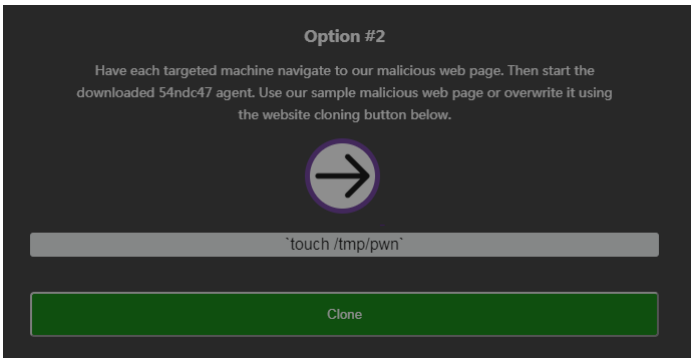
1c3z commented on Sep 2, 2019

login the caldera

open the url
http://127.0.0.1:8888/plugin/sandcat/gui

Enter a url, click clone button

```
`touch /tmp/pwn`
```




```
(env_caldera) [root@Recon tmp]# ls -al /tmp/pwn
-rw-r--r--. 1 root root 0 9月   2 18:01 /tmp/pwn
```

khyberspache commented on Sep 2, 2019 Contributor

Good catch. That makes sense considering how we clone the site... appears to truncate the wget command to allow arbitrary shell command execution. If you have a PR to fix this, feel free to submit.

privateducky added the bug label on Sep 6, 2019

ajunlee mentioned this issue on Sep 9, 2019

fix OS command injection in sandcat_gui_api mitre/sandcat#74

Merged

privateducky commented on Sep 20, 2019 Contributor

This appears fixed - closing (thanks **@ajunlee**)

privateducky closed this as completed on Sep 20, 2019

Assignees

No one assigned

Labels

bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants