HAWKTESTERS

AUGUST 2024

OS COMMAND INJECTION

CVE-2024-46330

PRESENTED BY

Table of Contents

Vulnerability Description

Presentation of CVE-2024-46330

Issue

Hawktesters identifies a vulnerability in the `VONETS VAP11G-300` router, This device makes use of the `doSystem` function which is a custom function of the `system` function in C language, allowing the execution of commands in the C language.

Mitigation

- To avoid command injection when passing arguments to a `system()` function in C, follow these recommendations:
- Avoid using system(): use specific functions such as `exec()` or `fork()` that offer more control and security.
- Strictly validate and filter user input.
- Escape characters such as ;, |, &, >, <, and \ that could be used for injections.

Versions Affected

The details can be seen in the following table.

Device Name	VAP11G_300
Hardware Version	VER6.0
Software Version	3.3.23.6.9 (Jun 9 2023 14:52:17)
Library Version	2022.11.23

Technical Description

Description

Vonets VAP11G-300 is a professional 300Mbps wifi bridge of small size that also performs the function of WiFi repeater. The new design is unique in the world and ensures long-lasting stability. It is based on IEEE 802.11n, IEEE 802.11b and IEEE 802.11g standards.

Issue(s)

Hawktesters has discovered a reverse-engineered command injection vulnerability in the `iptablesWebsFilterRun` component that allows the execution of operating system commands.

Proof of Concept

User Required: Yes

The `iptablesWebsFilterRun` object, which is used to execute iptables rules on the device, allows the injection of commands into the system, thus allowing control of the device to be taken.

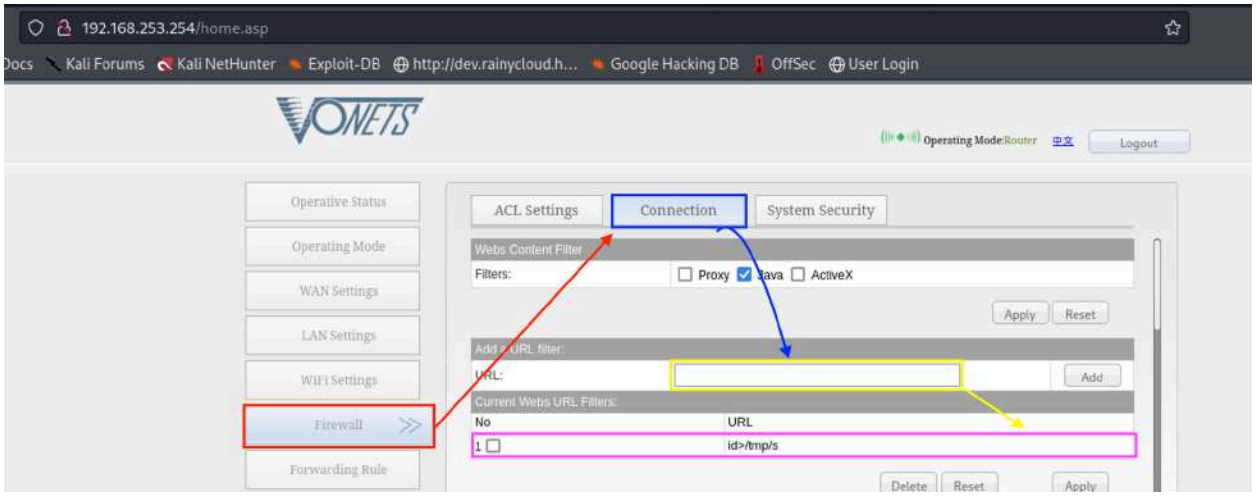
The code region that exposes the vulnerability is as follows:

```
doSystem("iptables -A web_filter -p tcp -m tcp -m webstr --url  %s -j REJECT --reject-with t cp-reset"
,local_128,uVar6,pcVar3);
```

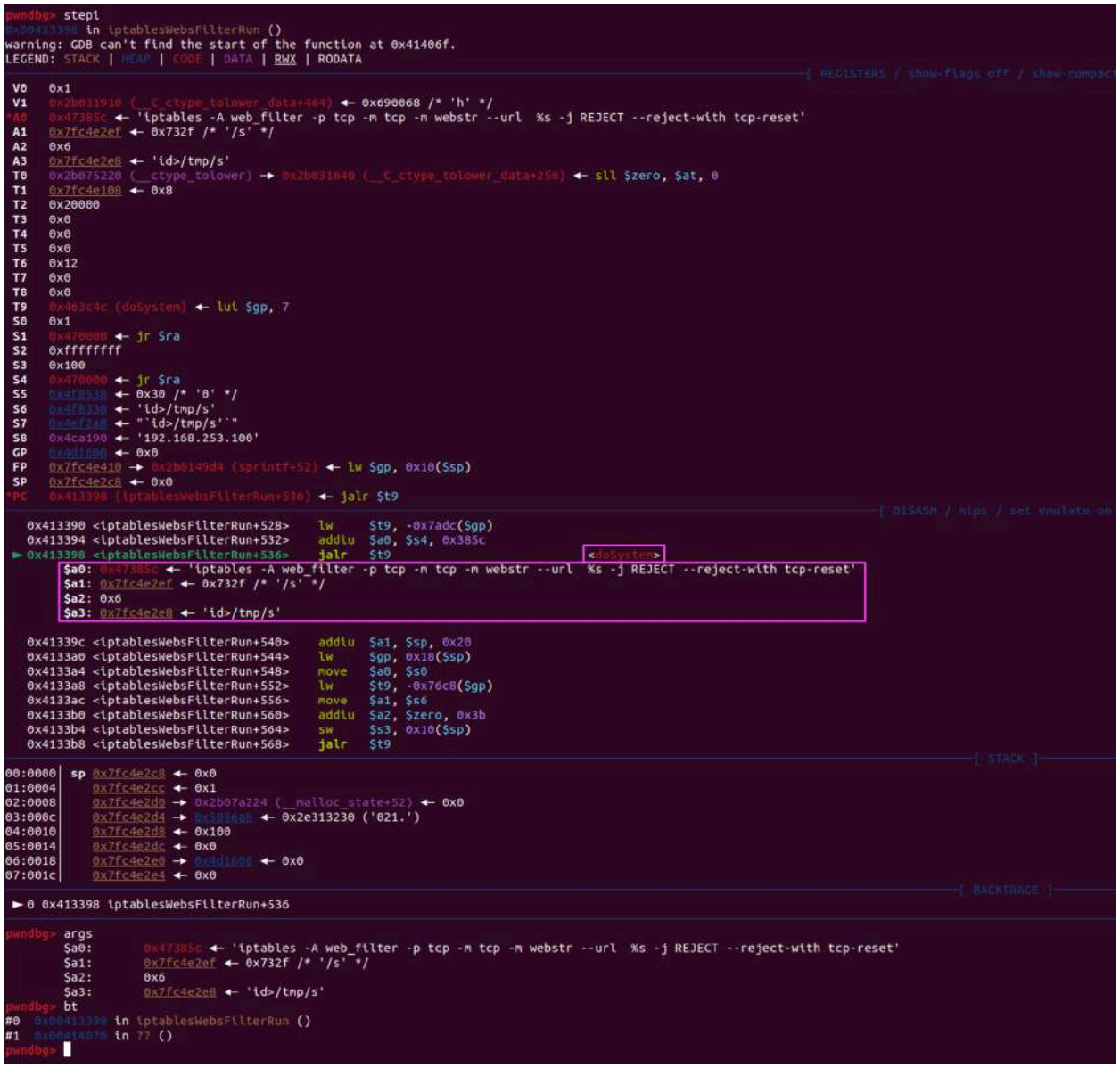
Command injection should be achieved by adding the following structure:

```
`COMMAND`
```

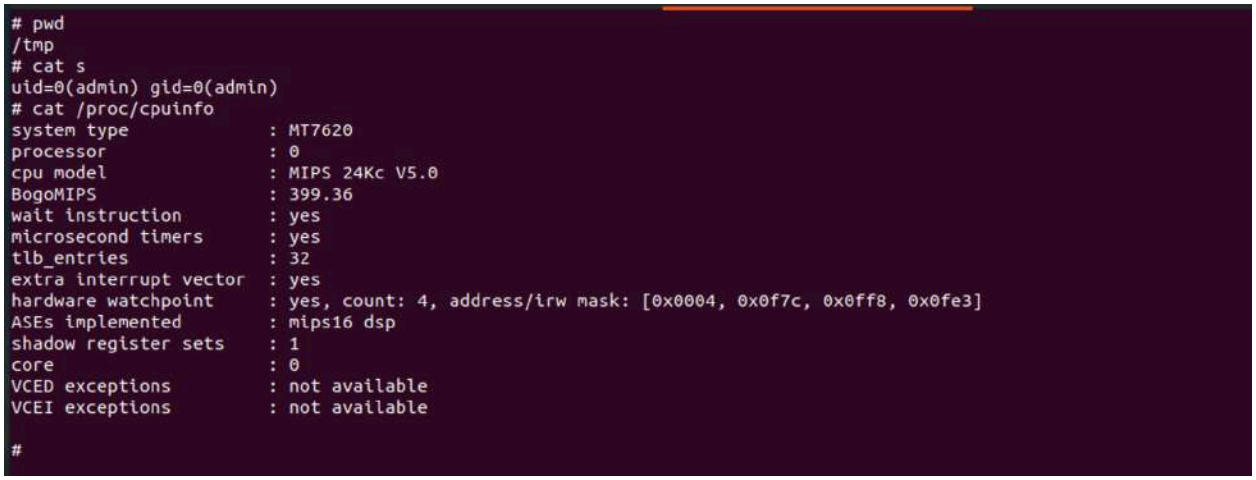
You can inject the code from here:



When the command is sent, manipulating the arguments, we can see the following:



Finally the injection is successful, by verifying the creation of the file.



Conclusions

Exploiting this vulnerability does not require extensive technical efforts, the scope of this vulnerability by allowing the execution of commands and taking control of the system makes it a critical attack vector for attackers.