Cr1pt0 Follow
Mar 20, 2021 · 2 min read · Listen

CVE-2020–28695

I have found a Remote Code Execution (RCE) vulnerability (CVE-2020–28695) on Askey Fiber Router, widely used in Brazil by the largest internet provider from this Country (Vivo Telefonica S.A). This vulnerability has already been fixed by the vendor.

The tested model was Askey Fiber Router RTF3505VW-N1 BR_SV_g000_R3505VWN1001_s32_7.

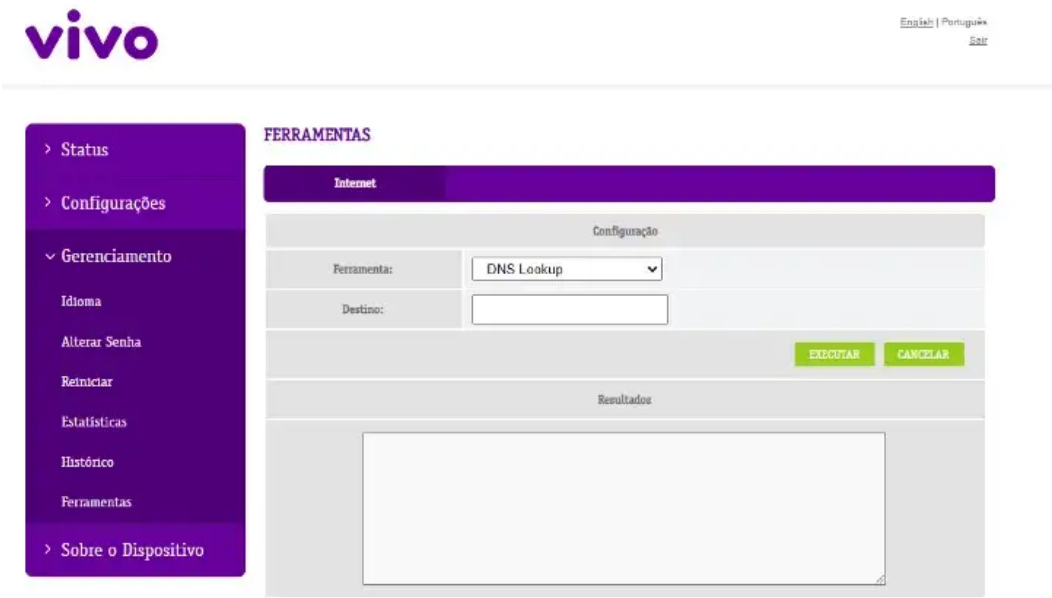
What is Remote Code Execution (RCE)?

Remote Code Execution (RCE) is one of the most dangerous types of computer vulnerabilities. It allows an attacker to remotely run malicious code within the target system on the local network or over the Internet. Physical access to the device is not required. An RCE vulnerability can lead to loss of control over the system or its individual components, as well as theft of sensitive data.

Proof of Concept (PoC)

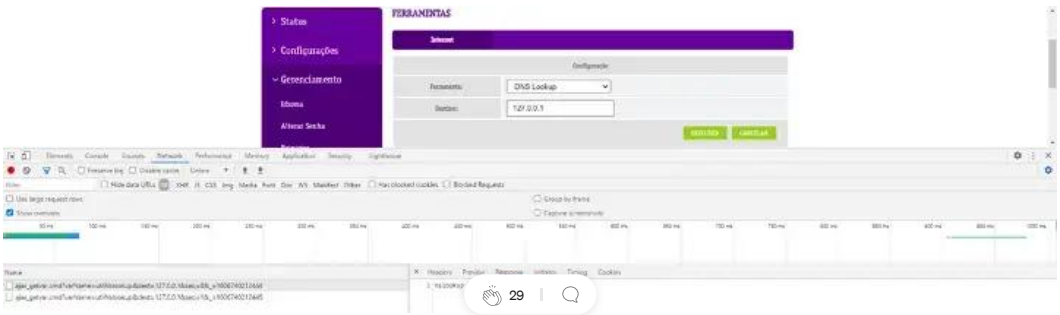
To exploit this vulnerability, the attacker must be connected to the router's network, either by Wi-Fi or wired connection.

The router has an Admin Dashboard, which contains some tools like Ping, DNS Lookup, Traceroute:

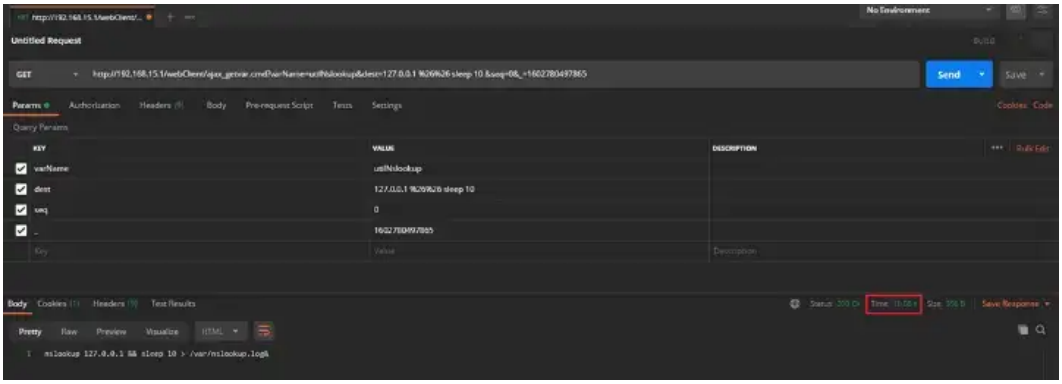


Router's Admin Dashboard

However, when we execute a tool, we can see that a Linux Command is being executed:

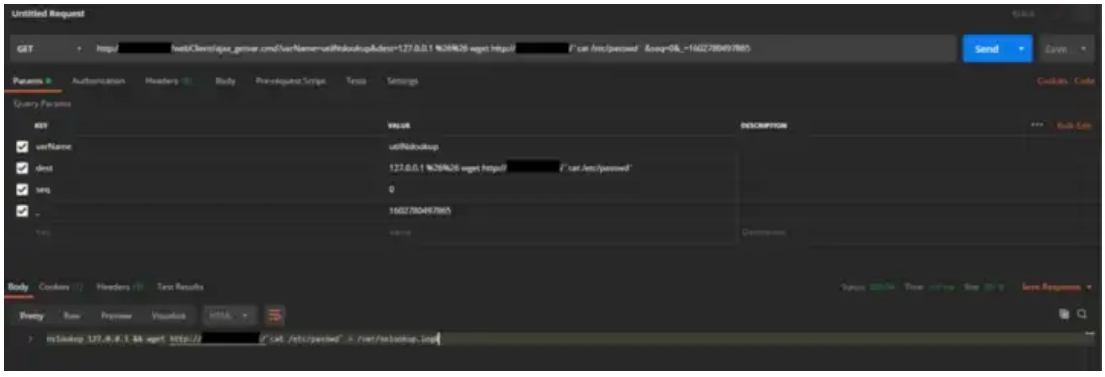


Then, I tried to inject some commands and the user input was not being sanitized. Therefore, I was able to run a SLEEP command in the router:



SLEEP command being executed in the router

For another PoC, I've started an HTTP Server on my local machine, and I executed a WGET on the router:



Wget executed on the router

So, I got the admin credential from the router:

Router's Admin Credentials

With these credentials, this vulnerability may even result in a Denial of Service (DoS), given that the attacker could:

- Change the Wireless password
- Change the router's admin password
- Modify the firewall rules
- Reboot the router
- Block the router's internet access

CVSS Base Score

CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H (8.8 High)

Mitigation

This vulnerability has already been fixed by the vendor. Vivo Internet S.A was notified and is aware of this vulnerability.

Cve Cve 2020 28695 Rce Vivo Poc