CVES

Copy

CVE-2022-33106

WiJungle Next Generation Firewall U250# Vendor Homepage: https://www.wijungle.com/# OS version: 9.4.9

```
# Exploit Title: WiJungle U250 NGFW - Brute-Force attack
# Category: Hardware
# Exploit Author: Harshit Rajpal
# Hardware Model: WiJungle Next Generation Firewall U250
# Vendor Homepage: https://www.wijungle.com/# OS version: 9.4.9
# CVE ID: CVE-2022-33106
# Date: 27.06.2022

##############################################################################
##########

Steps to Reproduce -

   - Navigate to the WiJungle login page situated at local IP
address.
   - Turn on the Burp Proxy. Add random username,password and
capture request.
   - Send the request to intruder and launch a sniper attack with
adding username and password in payload.
   - Try for most common usernames. You can use the file:
https://github.com/danielmiessler/SecLists/blob/master/Usernames/
top-usernames-shortlist.txt
   - Try for the most common passwords using various lists
available online.
   - Run the attack and you will find that the WiJungle NGFW has
a "NO RATE LIMIT" which allows a user to brute-force admin
credentials.
   - I compromised the admin credentials on an approx combination
of 30,000th payload.
```

Previous
CVEs

Next
Paper Reviews

Last updated 3 years ago