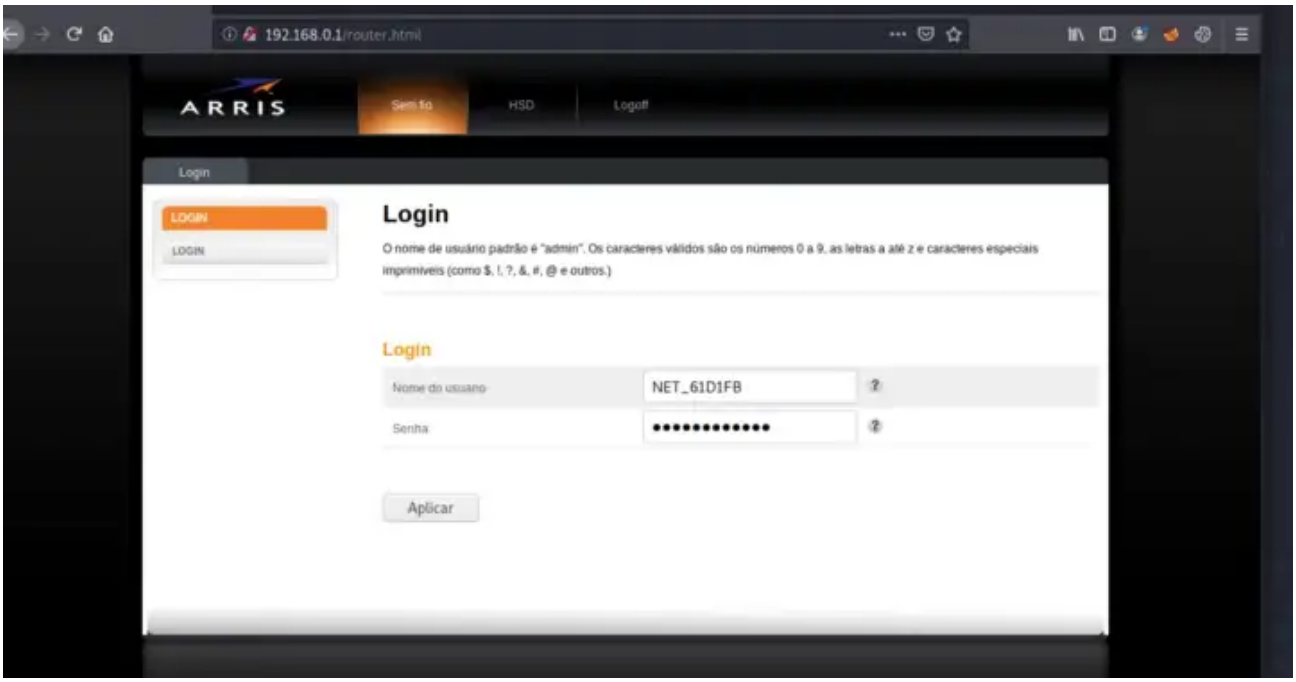
Rafael Silva
Follow
Feb 29, 2020 · 1 min read · Listen

Info disclosure — CVE-2020–9476

The Arris tg1692a router firmware 9.1.103DE2 does not sufficiently protect administrator credentials. The /login page discloses the administrator password in base64 encoding on the returned web page. A remote attacker can capture packets during the login process on this page and can obtain administrator credentials for the device.

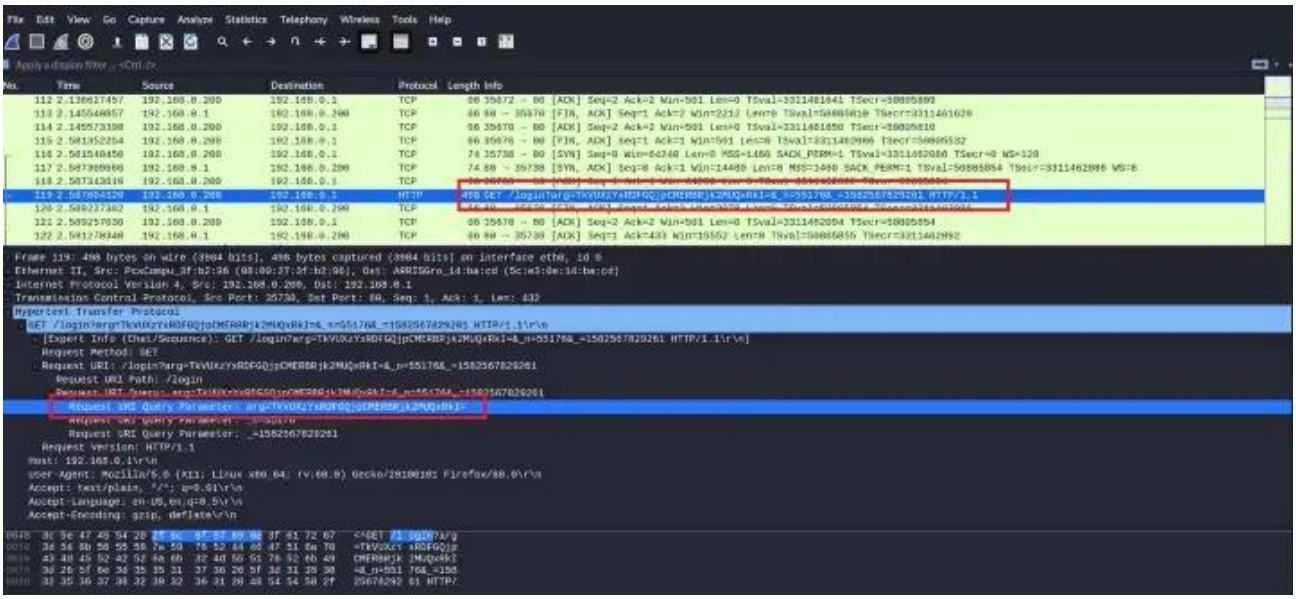
Proof Of Concept —
First Step —

Start packet capture then log in and password on the router.

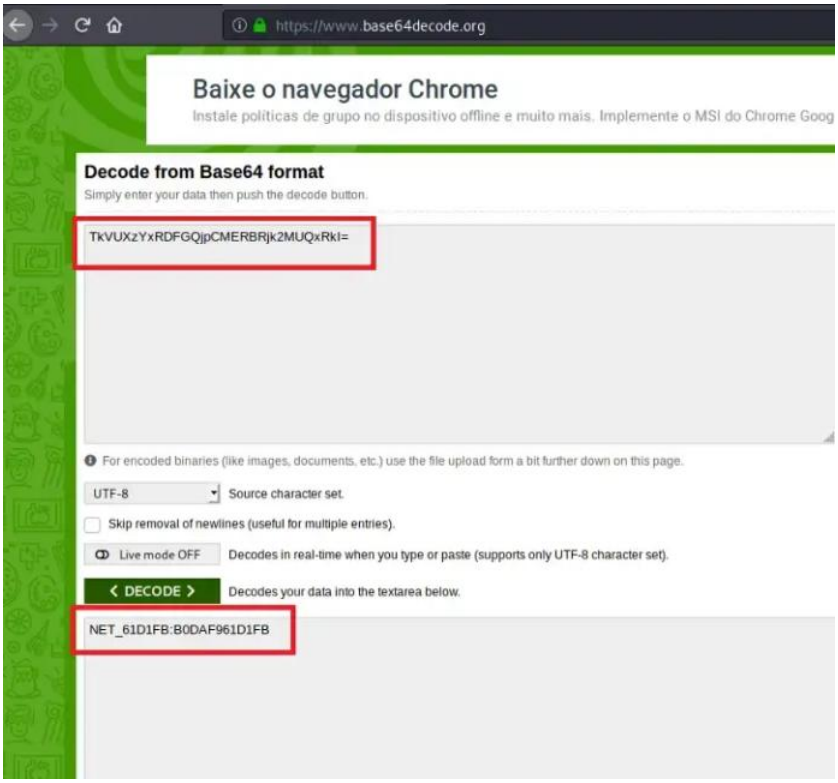


Second Step —

After the data capture, check the GET request on the / login page, the arg = parameter passes the login and password of the router encoded in base64.



After performing the base64 decode we have the login and password separated by: (colon)



Video —

https://vimeo.com/394691013