Rafael Silva Follow

Feb 29, 2020 · 1 min read · Listen

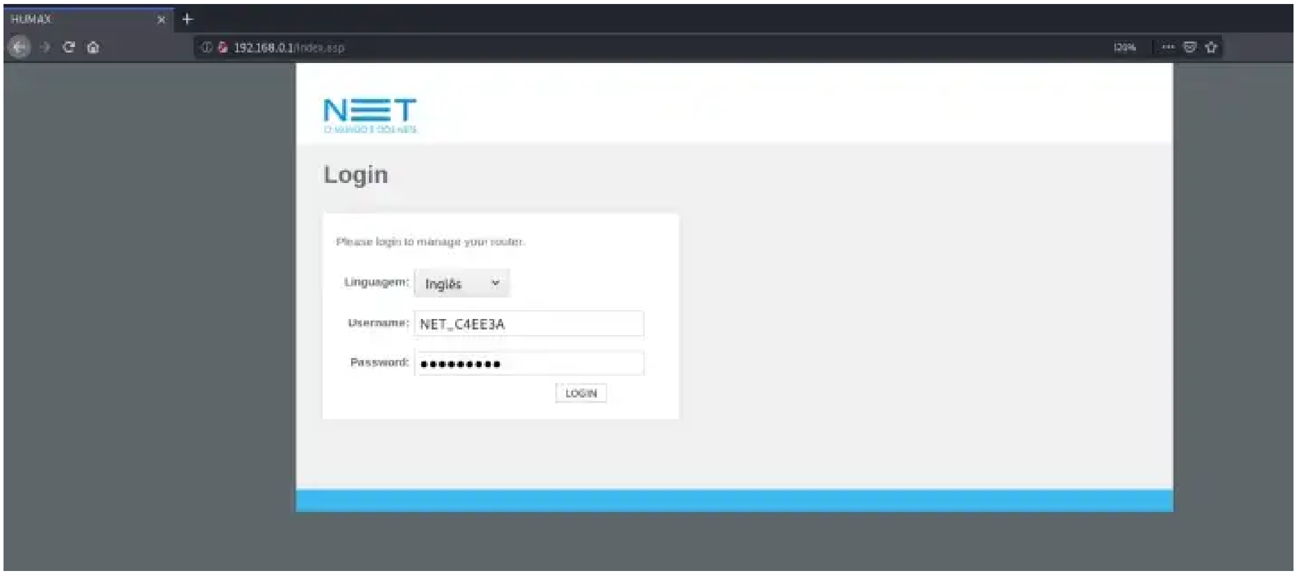
Save

Info disclosure — CVE-2020–9477

A vulnerability in the authentication functionality in the web-based interface of the HGA12R-02 router could allow an unauthenticated remote attacker to capture packets at the time of authentication and gain access to the plaintext password without any encryption. An attacker could use access to create a new user account or control the device.

Proof Of Concept —
First Step —

First start data capture during the router login process.



Login

Please login to manage your router.

Linguagem: Inglês

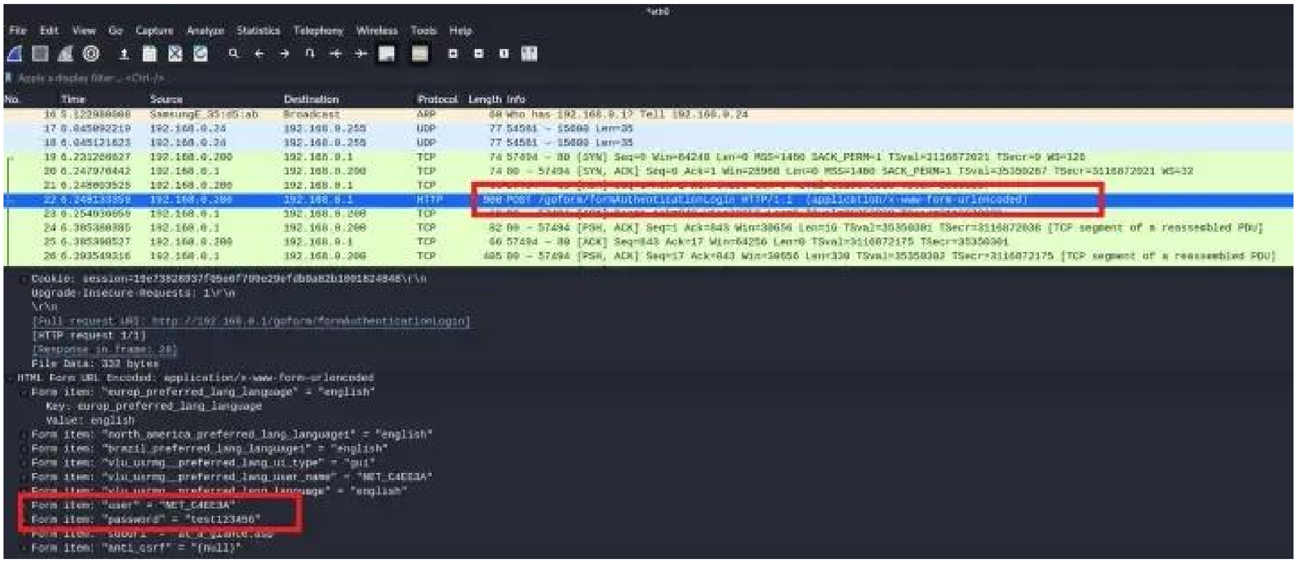
Username: NET_C4EE3A

Password: ●●●●●●●●●●

LOGIN

Second Step —

After the login you will verify in the data capture that you have access to the login and password in captured text.



*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time           Source              Destination      Protocol Length Info
  16 5.122980000    SamsungE_35:d5:ab   Broadcast        ARP        60 Who has 192.168.0.1? Tell 192.168.0.24
  17 6.045092219    192.168.0.24        192.168.0.255    UDP        77 54581 → 15600 Len=35
  18 6.045121823    192.168.0.24        192.168.0.255    UDP        77 54581 → 15600 Len=35
  19 6.231208827    192.168.0.200       192.168.0.1      TCP        74 57494 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3116872021 TSecr=0 WS=128
  20 6.247970442    192.168.0.1         192.168.0.200    TCP        74 80 → 57494 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=35350287 TSecr=3116872021 WS=32
  21 6.248003525    192.168.0.200       192.168.0.1      TCP        [illegible]
  22 6.248133350    192.168.0.200       192.168.0.1      HTTP      908 POST /goform/formAuthenticationLogin HTTP/1.1  (application/x-www-form-urlencoded)
  23 6.254030069    192.168.0.1         192.168.0.200    TCP        [illegible]
  24 6.385380385    192.168.0.1         192.168.0.200    TCP        82 80 → 57494 [PSH, ACK] Seq=1 Ack=843 Win=30656 Len=16 TSval=35350381 TSecr=3116872036 [TCP segment of a reassembled PDU]
  25 6.385380527    192.168.0.200       192.168.0.1      TCP        66 57494 → 80 [ACK] Seq=843 Ack=17 Win=64256 Len=0 TSval=3116872175 TSecr=35350381
  26 6.393549216    192.168.0.1         192.168.0.200    TCP       405 80 → 57494 [PSH, ACK] Seq=17 Ack=843 Win=30656 Len=339 TSval=35350382 TSecr=3116872175 [TCP segment of a reassembled PDU]
```

```
  Cookie: session=19e7382693 7f05e0f700e29efdb0a82b1001824848\r\n
  Upgrade-Insecure-Requests: 1\r\n
  \r\n
  [Full request URI: http://192.168.0.1/goform/formAuthenticationLogin]
  [HTTP request 1/1]
  [Response in frame: 26]
  File Data: 332 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "europ_preferred_lang_language" = "english"
    Key: europ_preferred_lang_language
    Value: english
  Form item: "north_america_preferred_lang_language1" = "english"
  Form item: "brazil_preferred_lang_language1" = "english"
  Form item: "vlu_usrmg__preferred_lang_ui_type" = "gui"
  Form item: "vlu_usrmg__preferred_lang_user_name" = "NET_C4EE3A"
  Form item: "vlu_usrmg__preferred_lang_language" = "english"
  Form item: "user" = "NET_C4EE3A"
  Form item: "password" = "test123456"
  Form item: "subUrl" = "at_a_glance.asp"
  Form item: "anti_csrf" = "(null)"
```

Video —

https://vimeo.com/394697339