xxy1126 / Vuln Public

Code Issues Pull requests Actions Projects Security Insights

main Vuln / 2 /

xxy1126 update 2022/8/17 … on Aug 16 History

..

readme.assets	3 months ago
readme.markdown	3 months ago

readme.markdown

TRENDnet TEW733GR contains Static Default Credential Vulnerability

overview

- type: static default credential vulnerability
- supplier: TRENDnet (https://www.trendnet.com/)
- product: TRENDnet TEW733GR
- firmware download: https://downloads.trendnet.com/tew-733gr/firmware/tew-733grv1_(fw1.03b01).zip
- affect version: TRENDnet TEW733GR v1.03B01

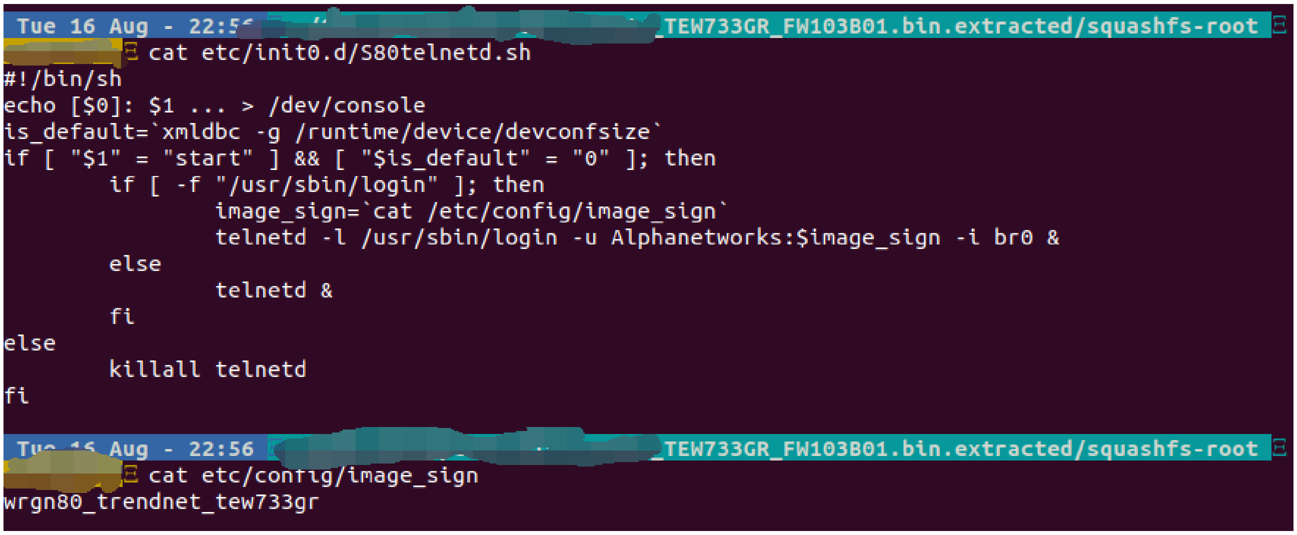
TRENDnet's N300 Wireless Gigabit Router, model TEW-733GR, offers proven high performance 300 Mbps Wireless N networking and gigabit wired Ethernet ports. Embedded GREENnet technology reduces power consumption by up to 50%. For your convenience this router comes pre-encrypted and features a guest network. Seamlessly stream HD video with this powerful router.

Description

1. Vulnerability Details

A vulnerability in the Telnet service of Trendnet 733GR could allow an unauthenticated, remote attacker to take full control of the device . The vulnerability exists because a system account has a default and static password. An attacker could exploit this vulnerability by using this default account to connect to the affected system. A successful exploit could allow the attacker to gain full control of an affected device.

In /etc/init0.d/S80telnetd.sh



```
 Tue 16 Aug - 22:5[redacted]_TEW733GR_FW103B01.bin.extracted/squashfs-root
[redacted] cat etc/init0.d/S80telnetd.sh
#!/bin/sh
echo [$0]: $1 ... > /dev/console
is_default=`xmldbc -g /runtime/device/devconfsize`
if [ "$1" = "start" ] && [ "$is_default" = "0" ]; then
        if [ -f "/usr/sbin/login" ]; then
                image_sign=`cat /etc/config/image_sign`
                telnetd -l /usr/sbin/login -u Alphanetworks:$image_sign -i br0 &
        else
                telnetd &
        fi
else
        killall telnetd
fi

 Tu[redacted] Aug - 22:56 [redacted]_TEW733GR_FW103B01.bin.extracted/squashfs-root
[redacted] cat etc/config/image_sign
wrgn80_trendnet_tew733gr
```

2. Recurring loopholes and POC

To reproduce the vulnerability, the following steps can be followed:

Start frimware through QEMU system or other methods (real device)

use the default username and password to login telnet