tj-oconnor / **CVE-2020-29001.txt** Secret

Last active 2 years ago

CVE-2020-29001

CVE-2020-29001.txt

```
1  ----------------------------------------
2  CVE-2020-29001
3  ----------------------------------------
4
5  [Suggested description]
6  An issue was discovered on Geeni GNC-CW028 Camera 2.7.2,
7  Geeni GNC-CW025 Doorbell 2.9.5,
8  Merkury MI-CW024 Doorbell 2.9.6, and
9  Merkury MI-CW017 Camera 2.9.6 devices.
10 A vulnerability exists in the RESTful Services API
11 that allows a remote attacker to take
12 full control of the camera with a high-privileged account. The
13 vulnerability exists because a static username and password are
14 compiled into the ppsapp RESTful application.
15
16
17 [Additional Information]
18 Contacted Merkury Innovations  on 21 Nov 20.
19
20 [Vulnerability Type]
21 Incorrect Access Control
22
23 [Vendor of Product]
24 Geeni
25
26 [Affected Product Code Base]
27 GNC-CW028 Camera - Version 2.7.2 (Current)
28 GNC-CW025 Doorbell - Version 2.9.5 (Current)
29 MI-CW024 Doorbell - Version 2.9.6 (Current0
30 MI-CW017 Camera - Version 2.9.6 (Current)
31
32
33 [Affected Component]
34 RESTful Web Application
35
36
37 [Attack Type]
38 Remote
39
40
41 [Impact Code execution]
42 true
43
44
45 [Attack Vectors]
46 An attacker is able to use the RESTful API to steal password hashes,
47 enable telnet service, gain access to stored audio/video files using
48 default/static credentials that are compiled into the RESTful web
49 application application.
50
51 [Discoverer]
52 TJ OConnor, Daniel Campos: Florida Tech IoT S&P Lab
53
54 [References]
55 https://research.fit.edu/media/site-specific/researchfitedu/iot-lab/Geeni_Disclosures.pdf
```