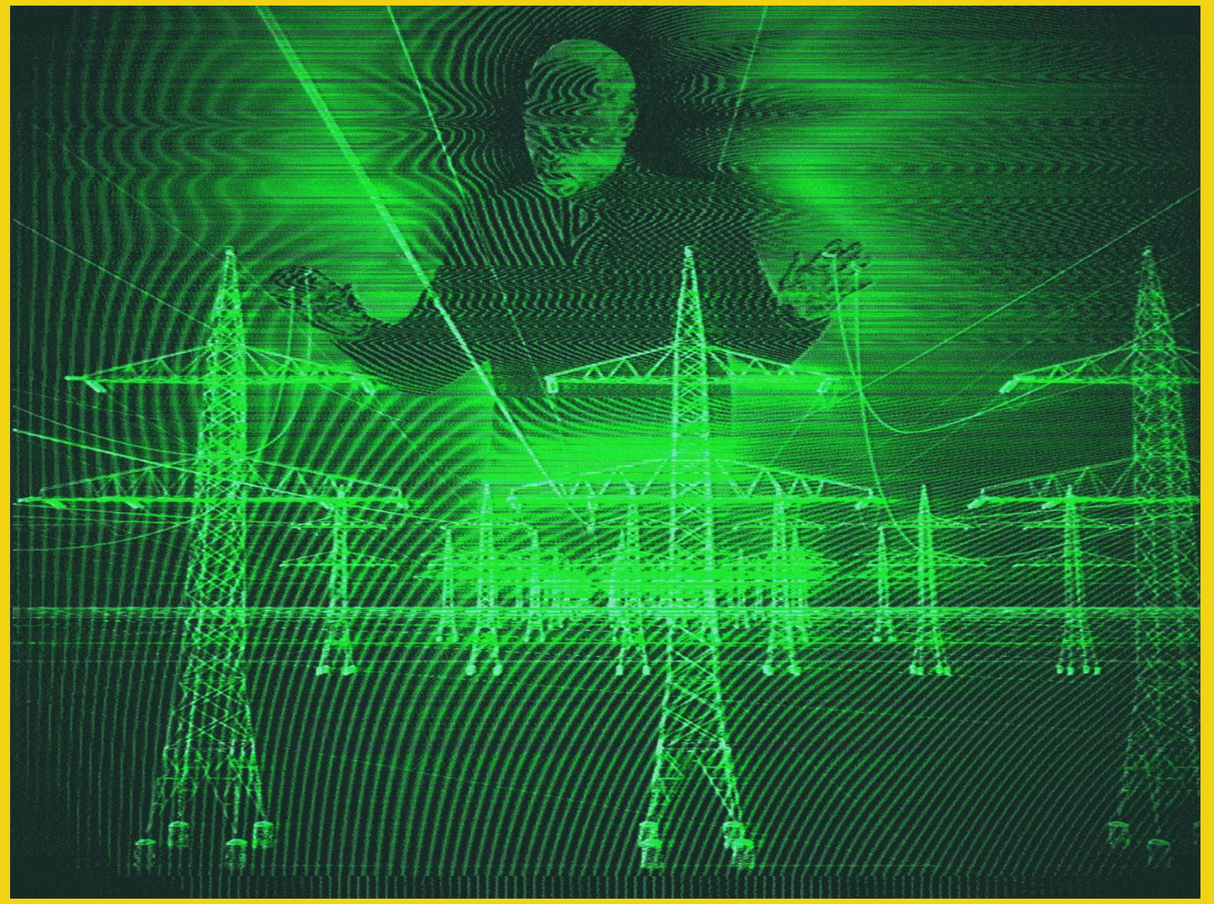
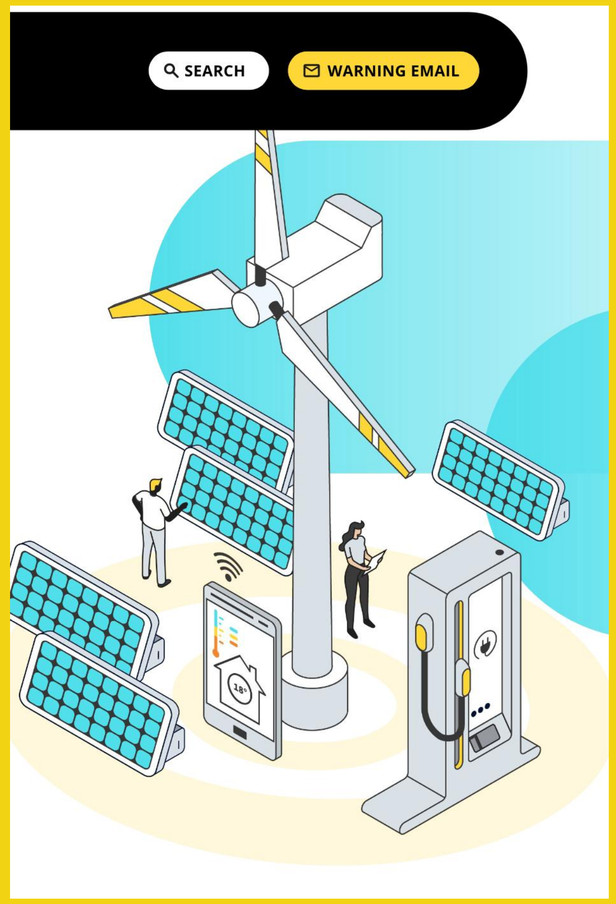
DIVD





Hoe wij het smart grid hacken om het veiliger te maken

Chris van ‘t Hof

IP 194.5.73.0-255 on your allow list, please

DIVD

Scan the internet for vulnerabilities

Reporting the vulnerability to the right people

0 Day disclosure

189	183	1.357.629
MEMBERS	TOTAL CASES	VULNERABLE IPS NOTIFIED

Mag dat?

Code of Conduct art. 4

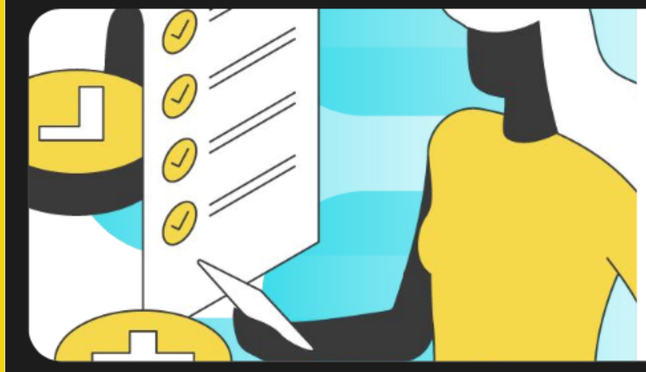
“DIVD doet echt buitengewoon goed werk en daar zijn we heel blij mee. Het NCSC werkt waar mogelijk met hen samen en zal dat blijven doen.”

Dilan Yeşilgöz,
MINISTER VAN JUSTITIE EN VEILIGHEID

Societal need: we do vulnerability disclosure to prevent online damage to as many internet users as possible and don’t serve any particular financial, political or individual interests.

Principle of Proportionality: we serve this need with appropriate means. Our research should increase and not decrease the integrity and availability of online systems.

Principle of Subsidiarity: if several means are available to meet the need, we opt for the one which has the least impact.



Ethics at the base of everything we do

We aim to make the digital world safer by reporting vulnerabilities we find in digital systems to the people who can fix them. We have a global reach, but do it Dutch style: open, honest, collaborative and for free.

CODE OF CONDUCT

Uitschakelen of brandgevaar

Hacker kon tienduizenden zonnepanelen saboteren door rondslingerend wachtwoord

Door Stan Hulsen · 24 juli 2022 · Aangepast: 25 juli 2022

RTL Nieuws

Tienduizenden zonnepaneelinstallaties in Nederland en een mi
kwetsbaar voor sabotage. Een Chinees bedrijf dat monitorings
levert, liet een wachtwoord voor een online-controlepaneel ro
Kwaadwillenden hadden de apparaten kunnen uitschakelen of
aanpassen, waardoor brandgevaar zou ontstaan.

DIVD

Beantwoording Kamervragen naar aanleiding van het artikel 'Hacker ontdekt dat Chinese zonnepanelen een bedreiging zijn voor ons stroomnet'

Kamerstuk | 02-09-2022

Minister Jetten (Klimaat en Energie) beantwoordt vragen naar aanleiding van het artikel 'Hacker ontdekt dat Chinese zonnepanelen een bedreiging zijn voor ons stroomnet'. De vragen zi
Kamerleden Rajkowski en Erkens (beide VVD).

↗ Beantwoording Kamervragen naar aanleiding van h
ontdekt dat Chinese zonnepanelen een bedreiging zij
stroomnet' (PDF | 9 pagina's | 419 kB)

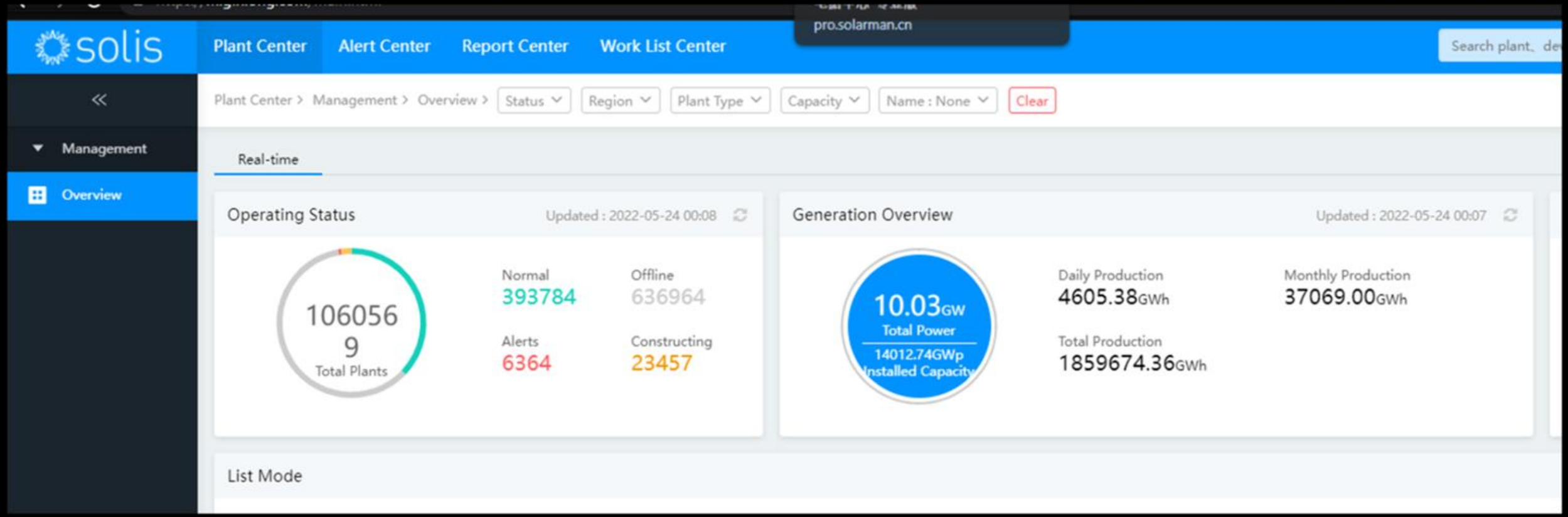
Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken en Klimaat

Rapport Rijksinspectie Digitale Infrastructuur

Onderzoek storingsproblematiek en cyberveiligheid omvormers voor zonnepanelen

Wat zou Vladimir, Xi of Donald kunnen doen met 10GW?

DIVD




Hack-out

12-6-2018
Hack de Grid

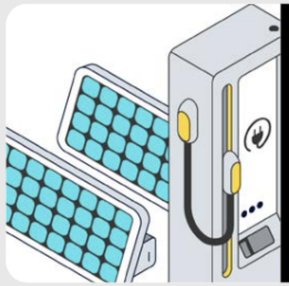
#hacktalk8

divd.nl/energie

DIVD

Wat gaan we precies doen?

Met het project CVD in de energiesector starten we een nieuwe onderzoekslijn om de digitale weerbaarheid van het steeds kwetsbaarder wordende energiesysteem te versterken. We richten ons op kennisontwikkeling, samenwerking en bewustwording binnen de sector en onderzoeken daarbij specifiek kwetsbaarheden in randapparatuur, zoals laadpalen, omvormers, thuisbatterijen en energiebeheersystemen. Eerdere bevindingen leidden al tot Kamervragen en acties van autoriteiten zoals de Rijksinspectie Digitale Infrastructuur (RDI).
In 2025 zetten we hierin de volgende stappen:



IoT Hacking Lab

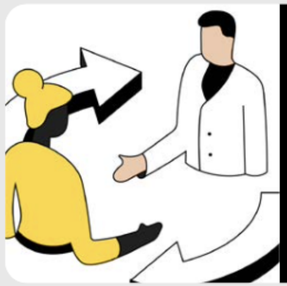
We zetten een IoT Hacking Lab op om onder andere randapparatuur zoals laadpalen, thuisbatterijen, omvormers e.d. te onderzoeken en testen. Daarnaast werken we samen met andere labs.

Onderzoek

We doen en publiceren onderzoek om hiermee autoriteiten en partners te ondersteunen bij handhaving en het implementeren van verbeteringen binnen de energiesector.

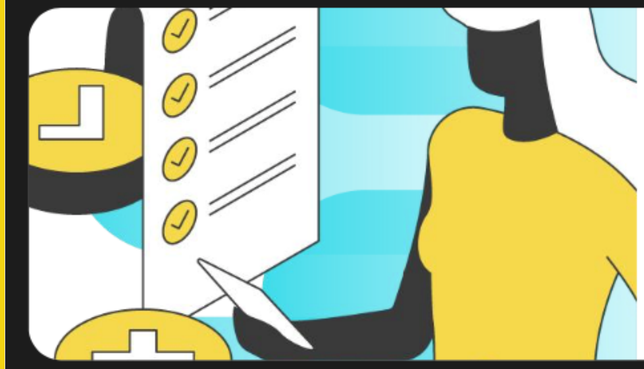
Educatie

We leiden nieuwe experts op met **DIVD. Academy** door lesmateriaal, trainingen en workshops te ontwikkelen voor studenten, de installatiebranche en onderwijsinstellingen in de energiesector.



Samenwerken

We werken samen met netbeheerders, overheden, leveranciers, fabrikanten, etc. om bewustzijn binnen de sector te vergroten en kwetsbaarheden te vinden en op te lossen.



Ethics at the base of everything we do

We aim to make the digital world safer by reporting vulnerabilities we find in digital systems to the people who can fix them. We have a global reach, but do it Dutch style: open, honest, collaborative and for free.

CODE OF CONDUCT

Scale up responsible disclosure to vendors

csirt.divd.nl/cna

DIVD

CVE Numbering Authority
(We can write in the global CVE database)

Hacker Wietse

CVE-2024-21876
CVE-2024-21877
CVE-2024-21878
CVE-2024-21879
CVE-2024-21880
CVE-2024-21881

DIVD

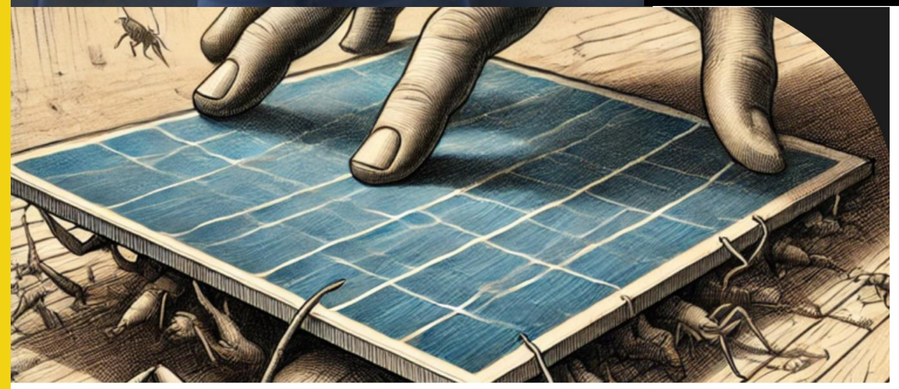
Why is it vulnerable?

```
def get_locale(use_qp=true)
   requested_locale = ""

   requested_locale = @cm.params['locale'][0].to_s if @cm.params.has_key?('locale')
   short_locale = requested_locale.slice(0,2)

   return requested_locale if @locales.has_key?(short_locale)
   return short_locale if @locales.has_key?(short_locale)
   return @@locale unless @@locale.empty?
   return get_emu_default_locale()[0]
end
```

HACKER HOTEL



DIVD responsibly discloses six new zero-day vulnerabilities to vendor

The Hague, Netherlands – Aug 12, 2024
by Serena de Pater and Marieke Smits

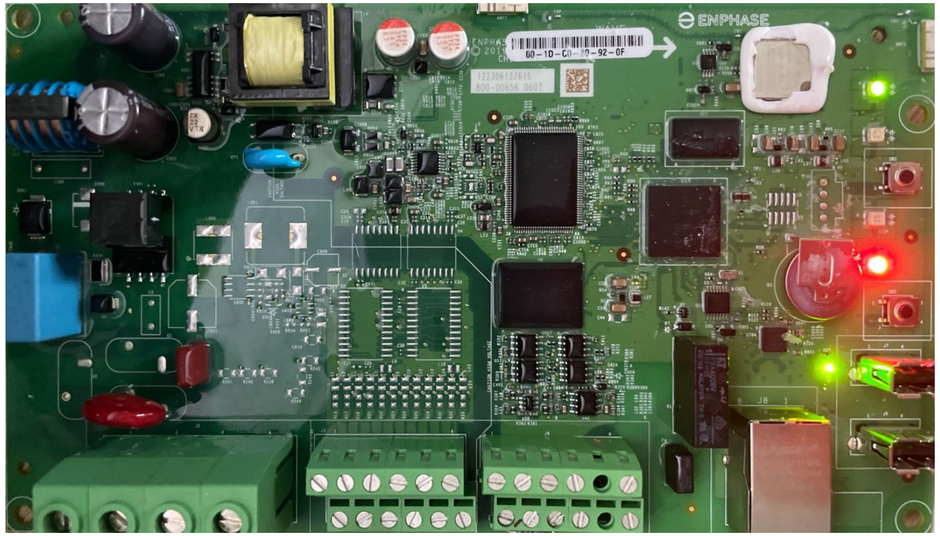
Case lead
Frank Breedijk

Researchers
Wietse Boonstra
Hidde Smit
Max van der Horst
Frank Breedijk

DIVD-2024-00011

About the case

DIVD researchers have discovered and, in collaboration with the vendor, disclosed **six new zero-day vulnerabilities** in Enphase IQ Gateway devices. This investigation was conducted by Wietse Boonstra and Hidde Smit, both researchers at DIVD, under case DIVD-2024-00011.



Hackers Harm& Wilco

CVE-2024-43648, CVE-2024-43649,
CVE-2024-43650, CVE-2024-43651,
CVE-2024-43652, CVE-2024-43653,
CVE-2024-43654, CVE-2024-43655,
CVE-2024-43656, CVE-2024-43657,
CVE-2024-43658, CVE-2024-43659,
CVE-2024-43660, CVE-2024-43661,
CVE-2024-43662, CVE-2024-43663

Press release: Research unveils 17 new zero-days in EV Chargers

In our most recent research into the security of EV chargers, 17 new vulnerabilities (zero days) were discovered in chargers manufactured by iocharger. These vulnerabilities were present in all AC-models of iocharger. The research was conducted by external researcher Wilco van Beijnum and DIVD researcher Harm van den Brink.

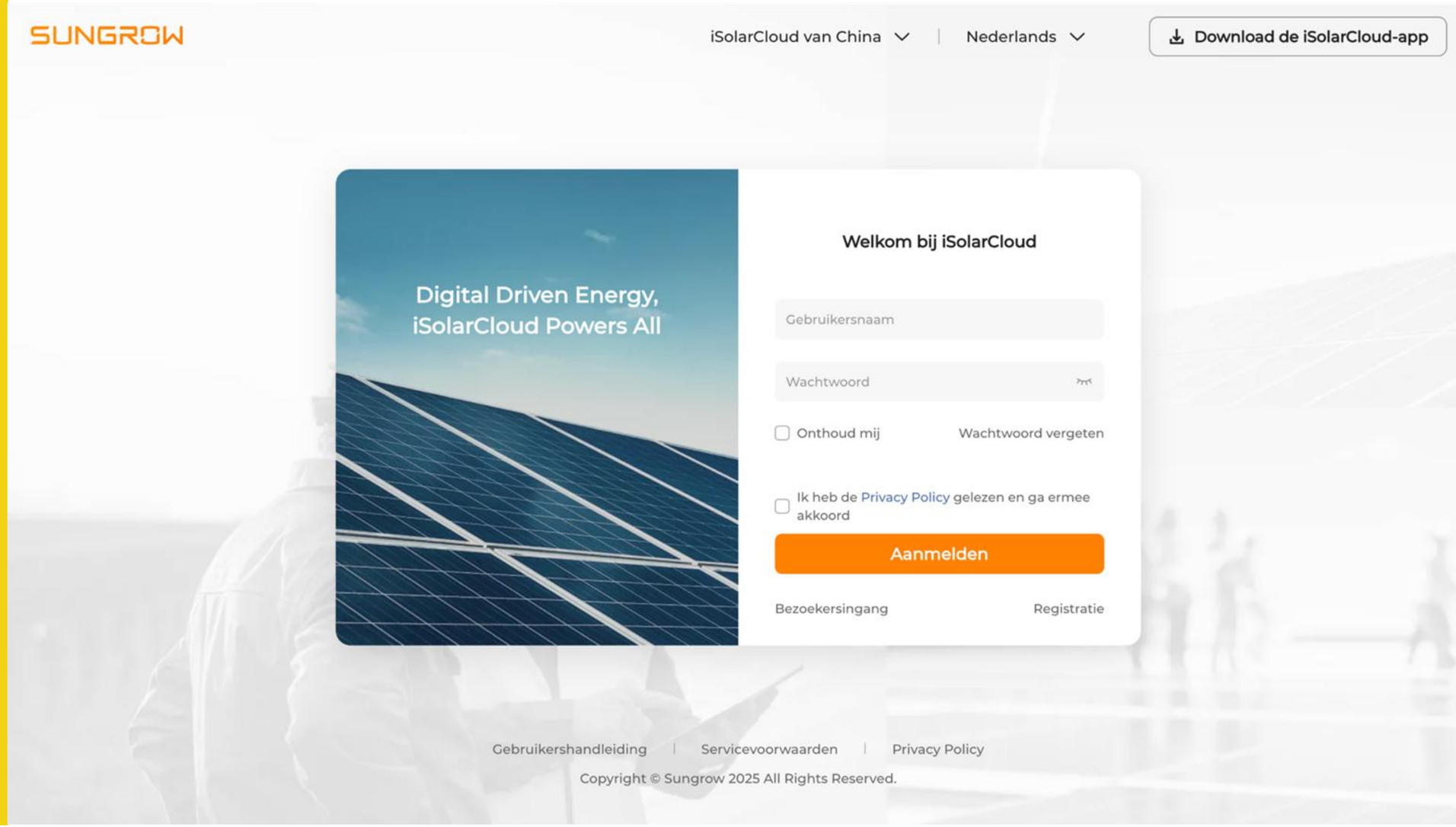
Case lead
Frank Breedijk

Researchers
Harm van den Brink
Wilco van Beijnum

DIVD-2024-00035

CVE-2025-29756

Disclosing 0-days



ENCS

DIVD

CVE-2025-29756

Disclosing 0-days

CVE-2025-29756

MQTT IMPLEMENTATION IN SUNGROW ISOLARCLOUD ALLOWED USERS TO SUBSCRIBE TO ALL DATA OF ALL CONNECTED INVERTERS

The credentials for the MQTT server as well as the RSA decryption key could be extracted from the javascript code and DOM of the iSolarCloud website. Using these credentials a malicious user could then subscribe to the # topic of the MQTT server and thus receive all data from all connected devices. Using the RSA decryption key obtained in the same manner all the messages from all topics could be decrypted as well.

Case lead	Frank Breedijk
Researcher(s)	• Harm van den Brink

DIVD

ENCS

CVE-2025-29757

Disclosing 0-days

DIVD-2025-00011 - FAILED AUTHENTICATION CHECK IN GROWATT PORTAL

Due to an error in the authentication feature of the `plant transfer` function in the cloud platform of Growatt (either https://oss.growatt.com or https://server.growatt.com) failed to check authorisation when transfering an account from one account to another. A malicious users with a (free) installer account, could assign any plant to his account without this being noticable by the end user, effectively allowing this attacker to control and turn off any installation in the platform.

An attacker that is able to connect a significant number of plants with sufficient power and switches then at the right timing would potentially be able to disrupt the power grid.

Researcher(s)	• Humza Ahmad (ENCS) • Frank Breedijk • Victor Pasman • Harm van den Brink

DIVD

ENCS

CVE-2025-36756
CVE-2025-36757
CVE-2025-36758
CVE-2025-36759

Disclosing 0-days

DIVD-2025-00015 - VARIOUS VULNERABILITIES FOUND IN SOLAX CLOUD PLATFORM FOR SOLARPANEL INVERTERS

A problem with missing authorization on SolaX Cloud platform allows taking over any SolaX solarpanel inverter of which the serial number is known.

It is possible to bypass the administrator login screen on SolaX Cloud. An attacker could use parameter tampering to bypass the login screen and gain limited access to the system.

It is possible to bypass the clipping level of authentication attempts in SolaX Cloud through the use of the 'Forgot Password' functionality as an oracle.

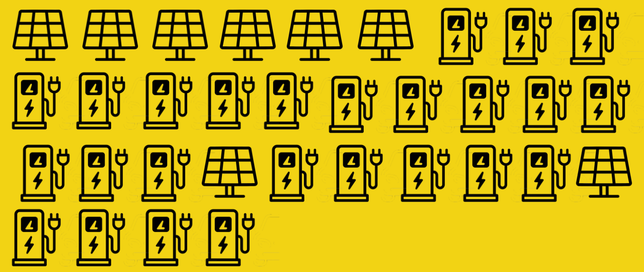
Through the provision of user names, SolaX Cloud will suggest (similar) user accounts and thereby leak sensitive information such as user email addresses and phone numbers.

Researcher(s)	• Humza Ahmad (External Researcher) • Harm van den Brink • Frank Breedijk • Max van der Horst

DIVD

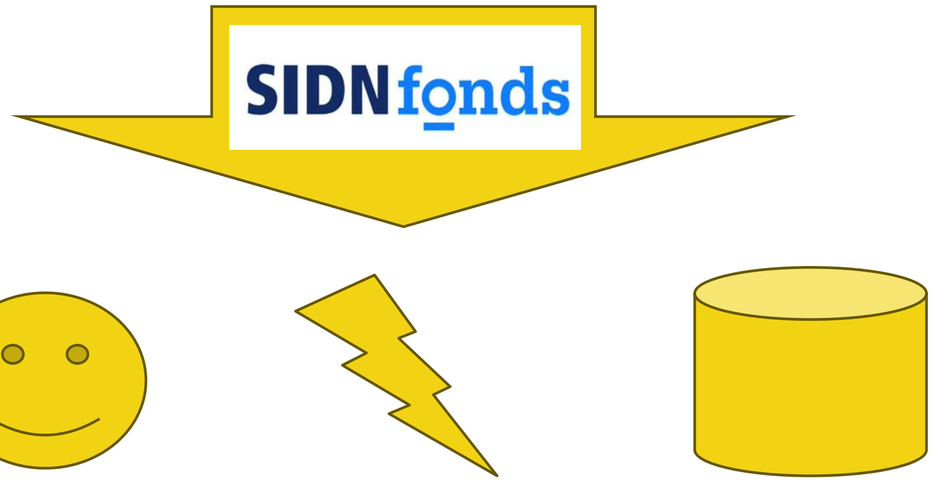
ENCS

Scale Up!



- Waiting for any kind of response from the vendor
- Vendor is it’s own CNA
- Waiting for vendor response
- Waiting for vendor response
- Waiting for vendor response
- Waiting for vendor response
- Waiting in line for more DIVD CNA admins
- Waiting in line for more DIVD CNA admins
- Waiting in line for more DIVD CNA admins

DIVD



RED

CRA

CBW

DIVD

Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken

Home › Onderwerpen › 6. Draadloze apparatuur › Apparatuur & richtlijnen

Cyber Resilience Act (CRA)

De Cyber Resilience Act (CRA) is een Europese verordening die zich richt op het verbeteren van de beveiliging van digitale producten. De CRA heet in het Nederlands de Verordening cyberweerbaarheid. De verordening is eind 2024 in werking getreden.

Omdat de CRA een verordening is, hoeft deze niet vertaald te worden naar Nederlandse wetgeving, maar is deze direct van kracht. Om nationale bevoegdheden te regelen, zoals de toezichtstaak van de RDI, is de Uitvoeringswet verordening cyberweerbaarheid opgesteld. Vanaf 11 december 2027 moeten alle producten met digitale elementen als inherent veilig ontworpen en geproduceerd zijn (zogeheten security-by-design). Daarnaast geldt voor fabrikanten en andere partijen in de toeleveringsketen een zorgplicht. Zij moeten bijvoorbeeld ondersteuning en beveiligingsupdates aanbieden en hebben een meldplicht bij kwetsbaarheden en incidenten.

Welke producten moeten aan de CRA voldoen?

Alle producten met digitale elementen moeten vanaf 11 december 2027 voldoen aan de CRA. Dit zijn niet alleen fysieke producten zoals IoT-apparatuur, firewalls of netwerkapparatuur. Denk ook aan software zoals videogames, mobiele apps en besturingssystemen zoals Windows. Ook componenten zoals videokaarten en software libraries vallen onder de CRA.

Wie krijgen met de CRA te maken?

Alle fabrikanten, importeurs en distributeurs van producten met digitale elementen krijgen te maken met de CRA. Daarnaast kunnen fabrikanten een vertegenwoordiger machtigen.

Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken

Home › Onderwerpen › 6. Draadloze apparatuur › Apparatuur & richtlijnen

Producenten en importeurs

Als producent of importeur van elektrische, elektronische of radioapparaten moet u ervoor zorgen dat uw producten voldoen aan de Europese richtlijnen: de EMC-richtlijn en Radio Equipment Directive (RED). Als een apparaat niet aan die eisen voldoet, is het illegaal om dit te produceren of verhandelen.

Wanneer bent u producent, fabrikant of importeur?

- U bent producent of fabrikant als u een product maakt of als u aan een bestaand product uw eigen merk geeft.
- U bent importeur als u een product koopt van een andere partij, afkomstig van buiten de EU (bijvoorbeeld uit China), en u het product binnen de Europese Economische Ruimte verkoopt.

Voor welke organisaties geldt de Cyberbeveiligingswet?

De Cyberbeveiligingswet geldt voor essentiële en belangrijke organisaties in verschillende sectoren, zoals energie, ruimtevaart, onderzoek, digitale infrastructuur en overheid. Ook grotere bedrijven in andere sectoren kunnen onder de wet vallen. Dit gaat bijvoorbeeld om bedrijven met meer dan 50 medewerkers, of met een jaaromzet en/of balanstotaal van meer dan 10 miljoen euro. Ook toeleveranciers of dochterbedrijven van zulke organisaties kunnen onder de wet vallen. Dit hangt af van hun rol in de keten.

Benieuwd of uw organisatie aan de Cwb moet voldoen?

Doe de NIS2-Zelfevaluatie

Hacking Demos

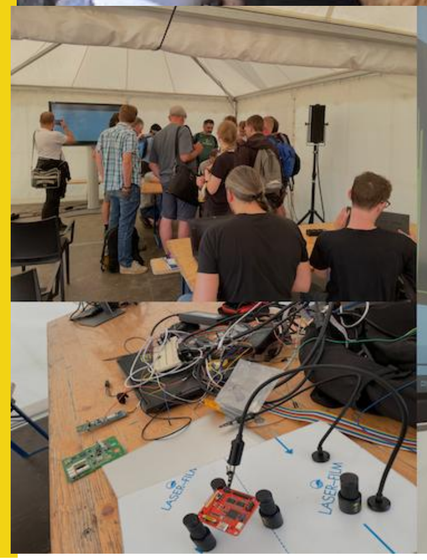
topsector energie

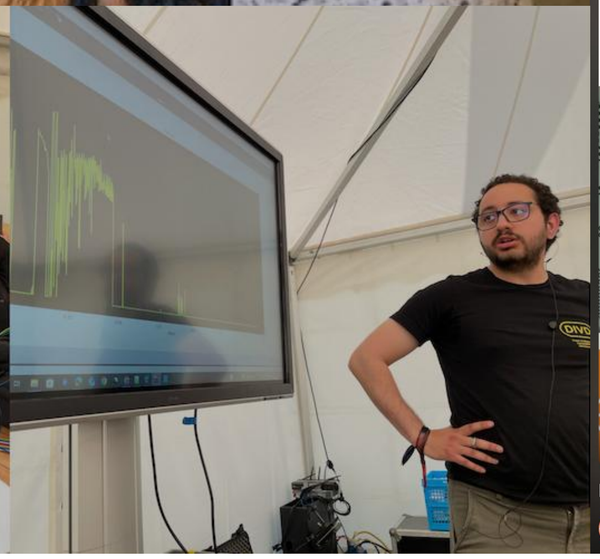
DIVD

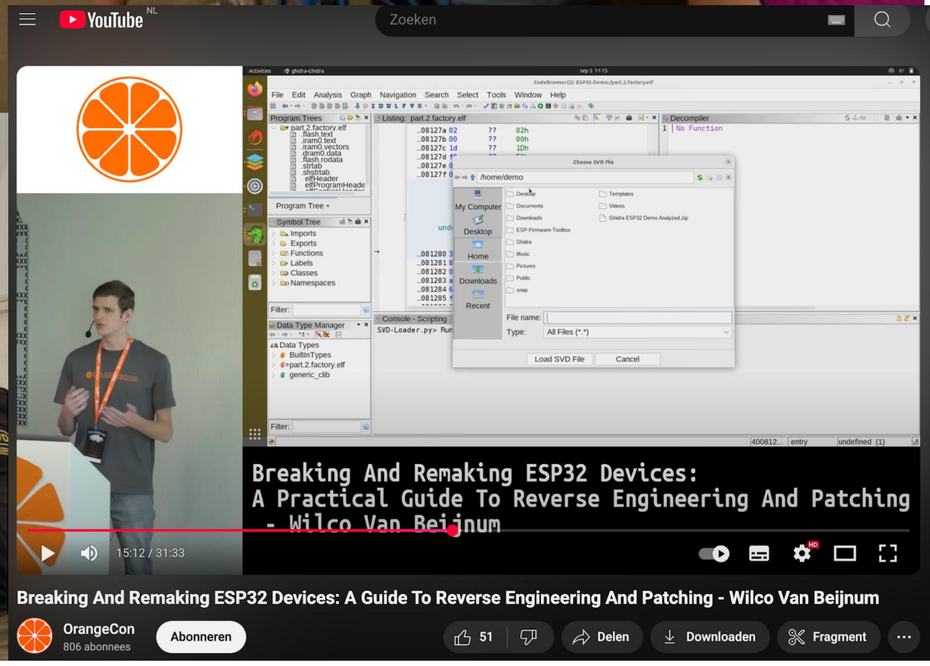
Hacking Demos

topsector energie

DIVD







Hacking Events

THE GREEN VILLAGE

THEMA'S INNOVATIES NIEUWS EN KENNIS FACILITEITEN OVER ONS

GEGEVENS

Begin:

11 november

Einde:

4 december

Evenement Categorieën:

Evenement, TGV, Toekomstig energiesysteem

Site:

https://www.aanmelder.nl/hack-the-power-...

LOCATIE

The Green Village

HACK THE POWER GRID

11 november - 4 december

Can you hack an energy management system at The Green Village?

As our power grid decentralizes, small weaknesses can have big consequences. Providers of energy management systems play a key role in protecting their systems and the wider grid from malicious attacks.

Are you **a student** who dares to take on **the challenge**? Outsmart professional white-hat hackers and compete for a total of **€4500 in prize money** across three categories. Lunch, snacks and drinks included

DIVD

THE GREEN VILLAGE

DIVD

Most Techy Hack

Wierdest Hack

Hardest Hack

1024 / 512






Technolution EMS
Technolution
THE GREEN VILLAGE



THE GREEN VILLAGE
DIVD
Dutch Institute for Vulnerability Disclosure


TU Delft
TUDelft
THE GREEN VILLAGE
SURF CERT
2025
CT
THE GREEN VILLAGE
AWARD
Hack the Pow
THE GREEN VILLAGE

DIVD

Divd.nl/energie

Samen voor een digitaal veilige energiesector

Met onze nieuwe onderzoekslijn versterken we de digitale weerbaarheid van het steeds kwetsbaarder wordende energiesysteem.

DOWNLOAD PARTNERDECK

Een slimme, duurzame, maar kwetsbare energiesector

Waarom veiligheid cruciaal is

Het Europese elektriciteitsnetwerk is nu een ‘smart grid’, waarin consumenten zowel energie gebruiken als produceren. Slimme online verbonden apparaten stemmen vraag en aanbod beter op elkaar af, wat verduurzaming en innovatie stimuleert. Tegelijkertijd maakt dit ons energiesysteem kwetsbaar voor digitale aanvallen. Hoewel losse apparaten weinig impact hebben, kan grootschalige manipulatie door cybercriminelen leiden tot ernstige stroomstoringen en zelfs een (inter)nationale black-out.

Join

DIVD

Nationaal Coördinator Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

THE GREEN VILLAGE

SIDN fonds

topsector energie

Elaad nl

ENCS

BUREAU VERITAS
Shaping a World of Trust

Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken

Zo kun je helpen

Financiën

Hoewel DIVD wordt gerund door bijna 200 Nederlandse vrijwilligers, hebben we financiële middelen nodig om ons werk effectief te blijven doen. Om continuïteit te waarborgen en te groeien, hebben we een stabiele financiering van minimaal €200.000 per jaar nodig. Dit stelt ons in staat te investeren in professionele ondersteuning, essentiële diensten, tools en medewerkers.

We zijn hierbij volledig afhankelijk van sponsoren en donateurs. Daarom zoeken we organisaties en individuen die ons willen steunen met terugkerende jaarlijkse donaties vanaf €5.000 per jaar.

Direct doneren, ga naar: **divd.nl/donate**

Materialen

Onze organisatie is sterk afhankelijk van IT. Gelukkig krijgen we al veel steun van leveranciers in de vorm van gratis licenties, tools en diensten.
Hoewel we geen productaanbevelingen doen – om onze ANBI-status en onafhankelijkheid te waarborgen – erkennen we graag een bijdrage op onze partnerpagina.

Daarnaast ondersteunen veel partners ons niet alleen op IT-gebied, maar ook met juridische, communicatieve en organisatorische expertise.

Mensen

Organisaties kunnen ons ondersteunen met de meest waardevolle hulpbron: mensen. Door medewerkers structureel een aantal uur per week de ruimte te geven om zich voor een langere periode in te zetten als vrijwilliger bij DIVD, dragen zij direct bij aan onze missie.

Dit draagt niet alleen bij aan hun persoonlijke ontwikkeling, maar laat ook zien dat hun werkgever onze missie ondersteunt en actief invulling geeft aan maatschappelijk verantwoord ondernemen.

Security researchers binnen de energiesector zijn meer dan welkom om zich als vrijwilliger bij DIVD aan te sluiten.

DIVD

chris@divd.nl

Q&A

www.divd.nl/energie


HAPPY
ENDING

H4CK3R$

z13N

D1Ng3N

4Nd3R$

d4N

4Nd3R3N

<insert happy end here>

<insert happy end here>

<insert happy end here>

Store & Deliver

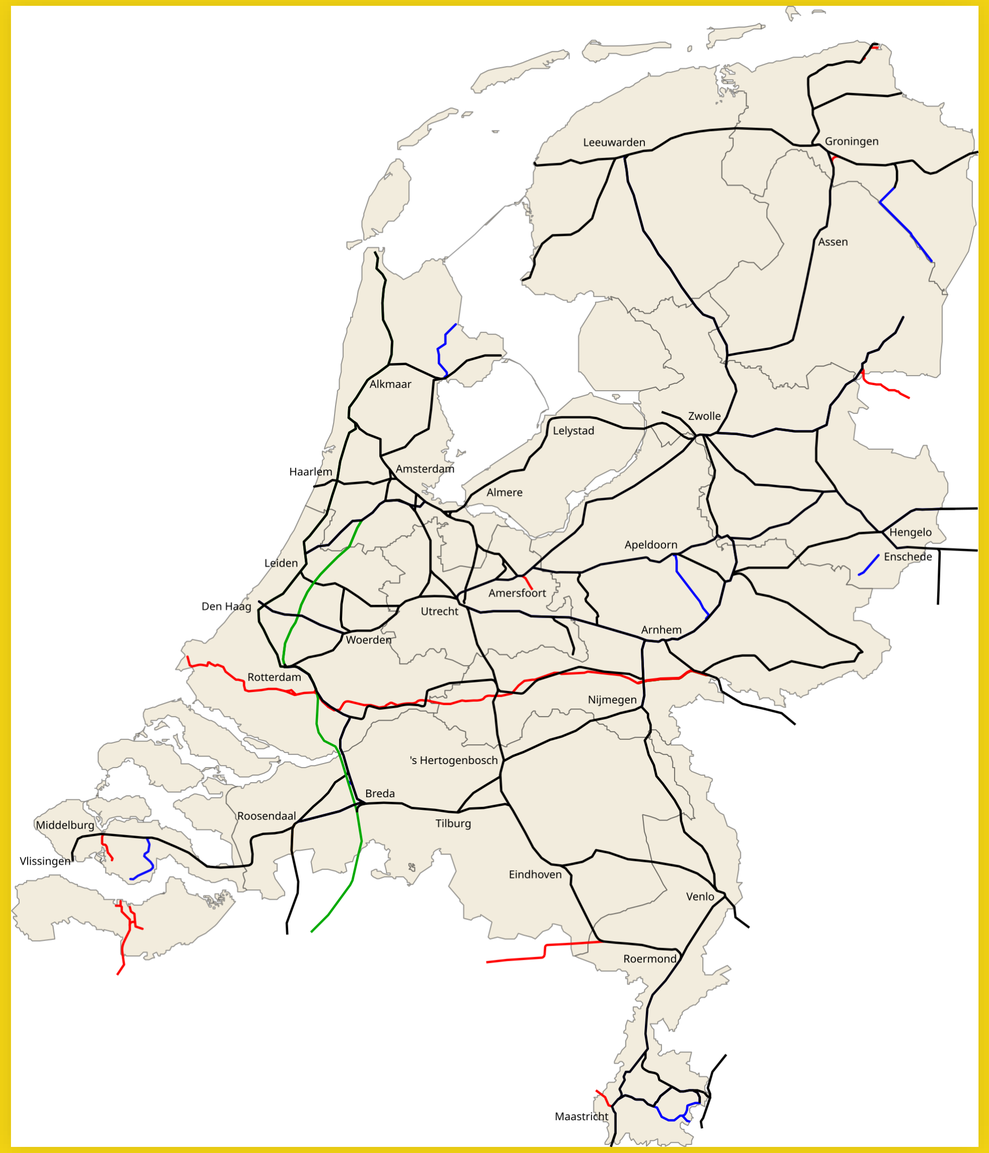
DIVD

Net binnen Algemeen Economie Sport Media en Cultuur Achterklap Shop Meer

Maandag 7 april 2025 | Het laatste nieuws het eerst op NU.nl

Een nationaal gelijkstroomnet

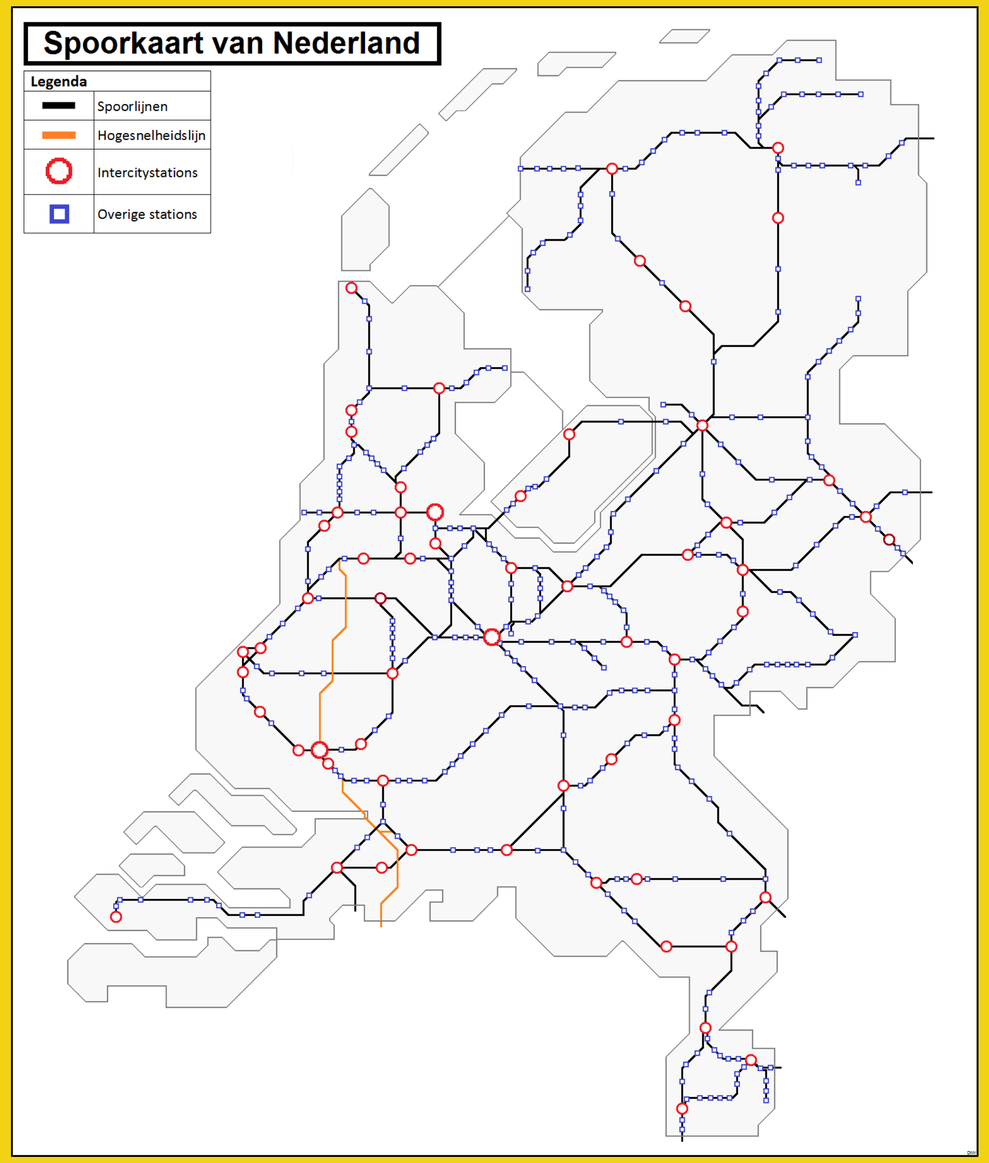
- Topologie: mesh netwerk
- Vermogenselektonica i.p.v. trafo
- 5, 14, 230 en 1.500 Volt



Een nationaal gelijkstroomnet

- Topologie: mesh netwerk
- Vermogenselektronica i.p.v. trafo
- 5, 14, 230 en 1.500 Volt
- 1,2 TWh/J=1.200.000.000 KWh = 500.000 pers.
- BV met NL Staat als grootaandeelhouder

DIVD



DIVD

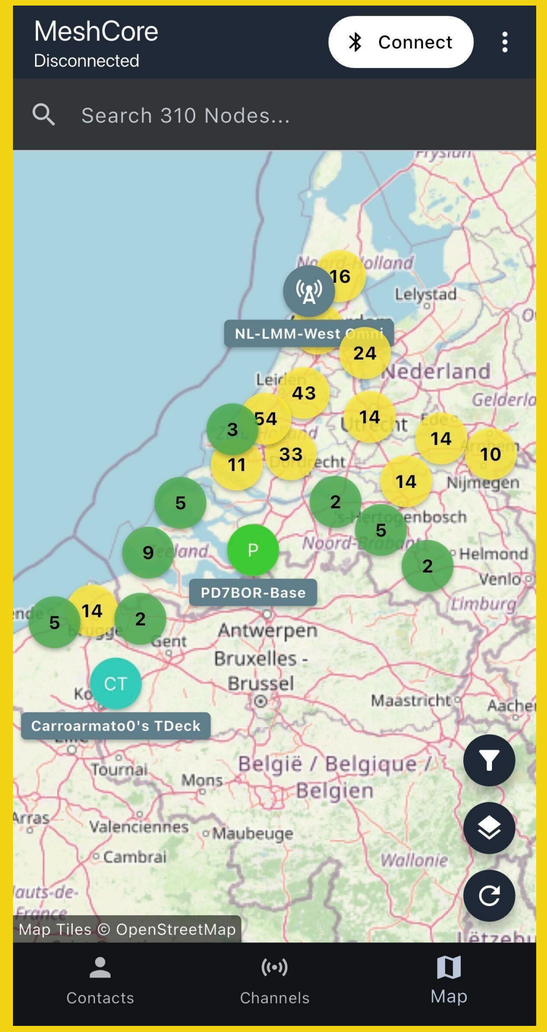
1 13

Uit de Kom @UitDeKom · Dec 14, 2024
#nietmijnoorlog #bankrun

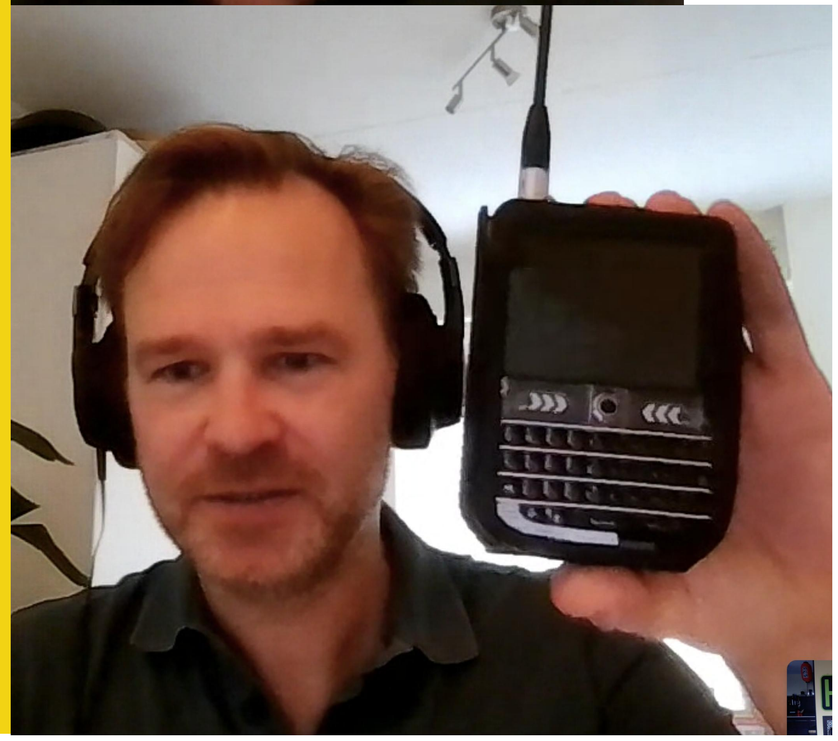
5 23 3.7K

Zappa-IsTheBest ⚓ @ZappaforPotus · Dec 15, 2024
Wie stopt deze oorlogshitser. #nietmijnoorlog

Join


MeshCore
Disconnected
Connect
Search 310 Nodes...
NL-LMM-West Omni
PD7BOR-Base
Carroarmato0's TDeck
Map Tiles © OpenStreetMap
Contacts
Channels
Map

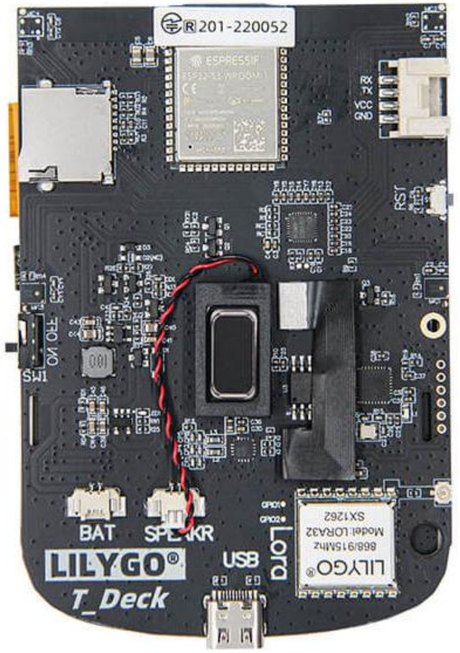
DIVD




Powered
RAK
RAK


Powered


Tx
Rx
Message
TX 33 finished
Radio Configure
Sour
ispla
GPS
KB
TING
LILYGO®


R 201-220052
BAT
SPEAKR
USB
LILYGO®
T_Deck
Lora


Hack-out
2026
(This is a drill)