



Dutch Institute for
Vulnerability
Disclosure

How We Hack the Power Grid to Make it Safer

Chris van 't Hof, 8 October 2026

We are DIVD: 180 helpful hackers and 40 partner organisations with a mission



Dutch Institute for
Vulnerability
Disclosure



Mission



Dutch Institute for
Vulnerability
Disclosure

We aim to make the digital world safer
by reporting vulnerabilities we and our partners
find in digital systems to the people who can fix them.

And we do this Dutch style:
open, direct and for free

We are the voluntary firebrigade of the internet

Vision



Dutch Institute for
Vulnerability
Disclosure

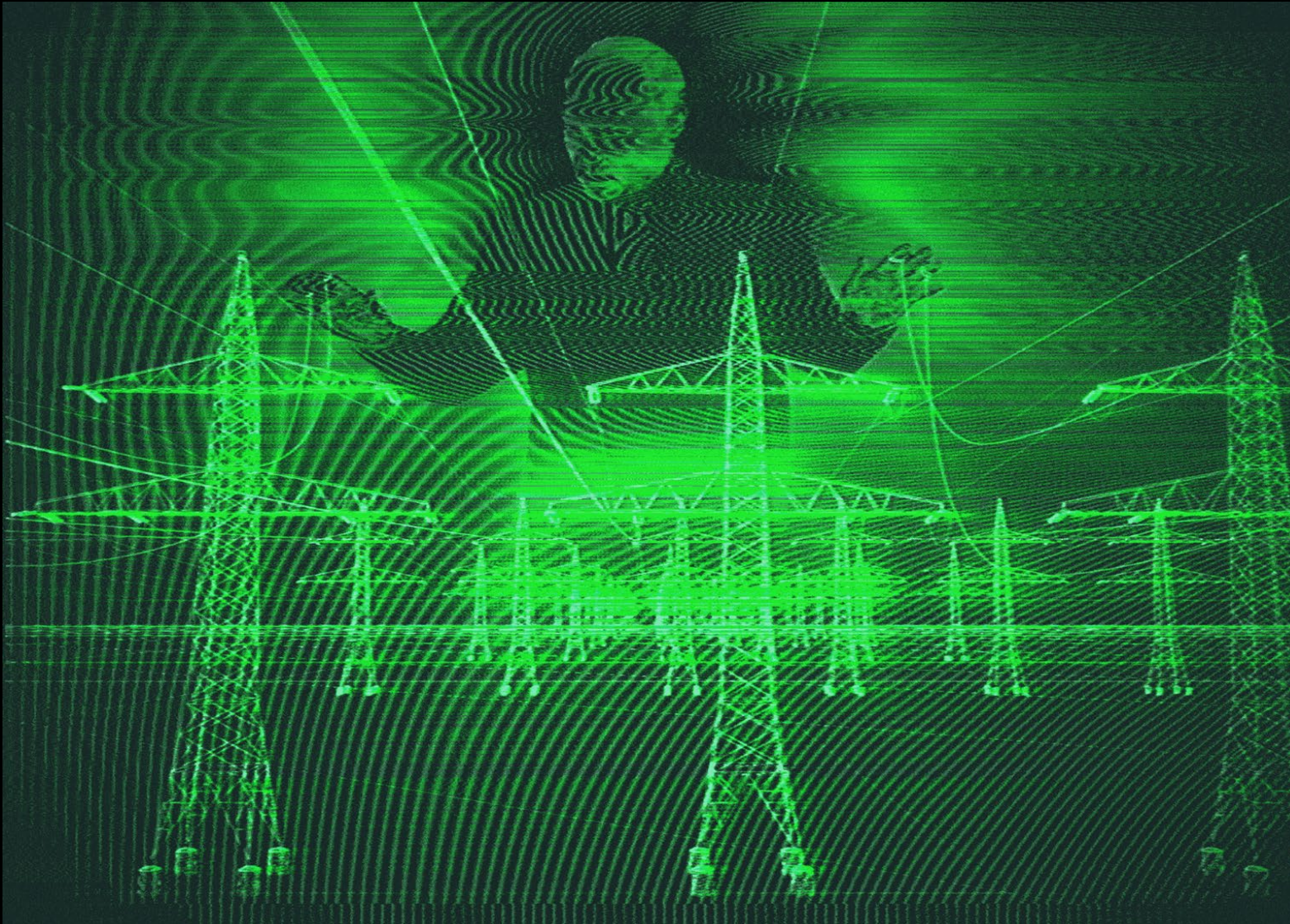
DIVD is a place
where helpful hackers
can do their thing,
free and safe.

We have been helping you for 7 years now



201 CVEs - > IPv4 scanned - > 1.433.803 notifications
176 Zero-days - > processed as CNA - > CVEs
1.379.844.098 stolen credentials processed - > notified
1 serious attack
0 law suits

(For just 400.000,- euro / year)



Dutch Institute for
Vulnerability
Disclosure

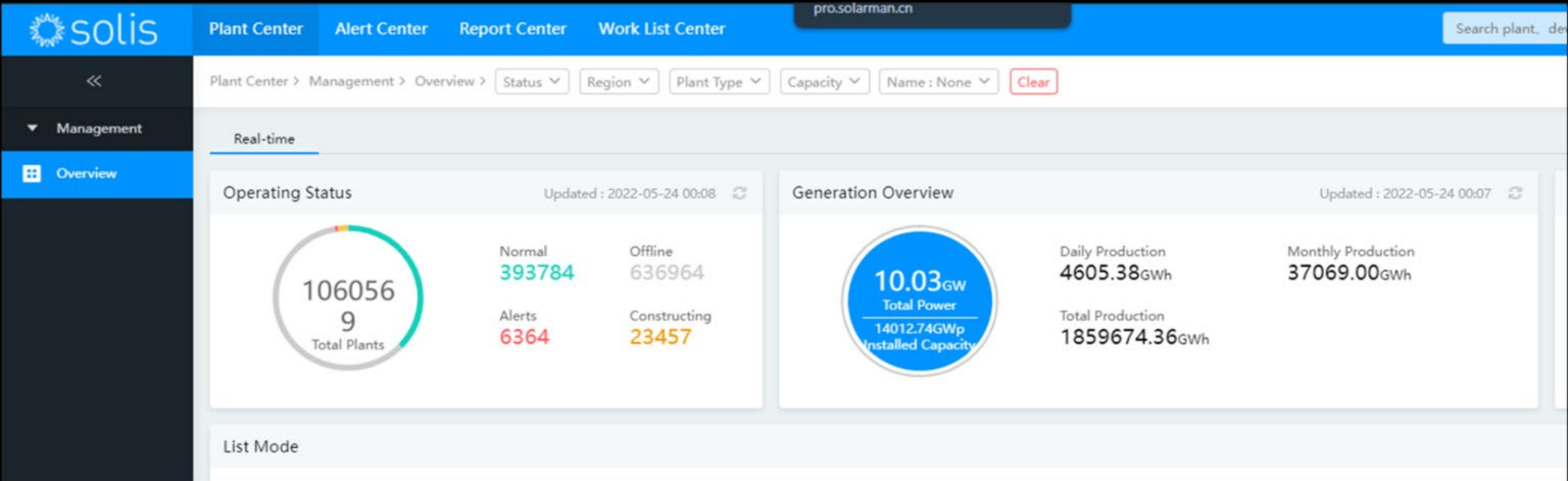
How someone could have turned Europe dark

With just one password...

What could you do with 10 GW?



Dutch Institute for
Vulnerability
Disclosure



An aerial photograph of a city at night, heavily tinted with a dark blue color. The image shows a dense urban landscape with numerous buildings, streets, and some green spaces. The lighting is dim, with some lights from the buildings visible. The overall mood is mysterious and tech-oriented.

Hack Out

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 miljoen woningen zijn kwetsbaar voor sabotage. Een Chinees bedrijf dat monitoringssoftware levert, liet een wachtwoord voor een online-controlepaneel rondslingeren. Kwaadwillenden hadden de apparaten kunnen uitschakelen of de software aanpassen, waardoor brandgevaar zou ontstaan.



Dutch Institute for
Vulnerability
Disclosure

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 zijn gesteld door Kamerleden Rajkowski en Erkens (beide VVD).

➔ [Beantwoording Kamervragen naar aanleiding van het artikel 'Hacker ontdekt dat Chinese zonnepanelen een bedreiging zijn voor ons stroomnet'](#) (PDF | 9 pagina's | 419 kB)



Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken
en Klimaat

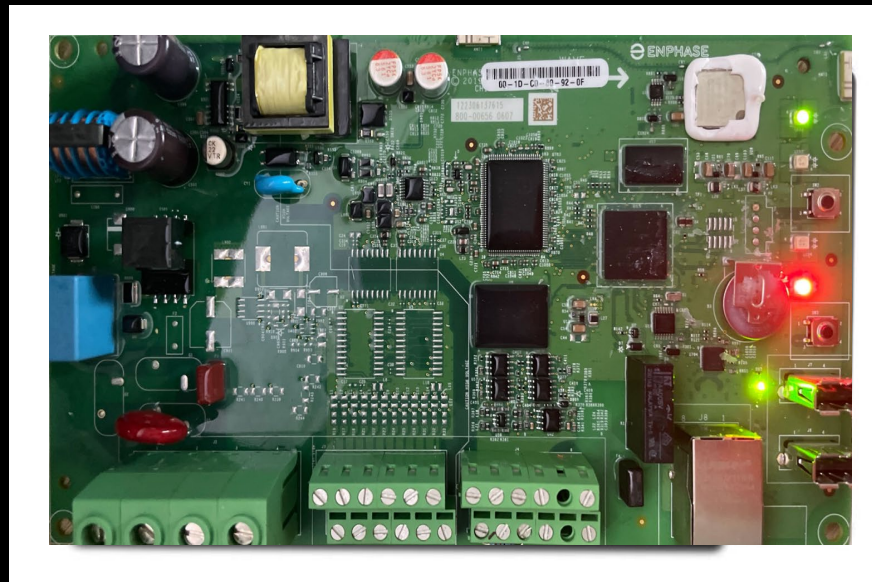
Rapport Rijksinspectie Digitale Infrastructuur

Onderzoek storingsproblematiek en cyberveiligheid
omvormers voor zonnepanelen

That's too easy, lets try harder



Dutch Institute for
Vulnerability
Disclosure

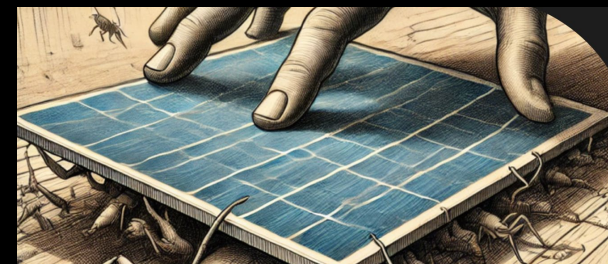


Why is it vulnerable?

```
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
```



DIVD responsibly discloses six new zero-day vulnerabilities to vendor

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

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.

Case lead
[Frank Breedijk](#)

Researchers
[Wietse Boonstra](#)
[Hidde Smit](#)
[Max van der Horst](#)
[Frank Breedijk](#)

[DIVD-2024-00011](#)

Time to scale up as a CVE Numbering Authority



Dutch Institute for
Vulnerability
Disclosure



csirt.divd.nl/cna



Dutch Institute for
Vulnerability
Disclosure



[About](#)[Partner Information](#)[Program Organization](#)[Downloads](#)[Resources & Support](#)[Report/Request](#)

Search

Site Search 

Search tips  | [Provide feedback](#) 

**Notice:** Expanded keyword searching of CVE Records ([with limitations](#)) is now available in the search box above. [Learn more here](#) .

NOTICE — Due to routine maintenance, this [CVE.ORG website](#) will be **unavailable on June 29, 2026, between 10:30 AM and 11:30 AM EDT**. We apologize for the inconvenience and thank you for your understanding.

CVE Numbering Authorities (CNAs)

CNAs are vendor, researcher, open source, CERT, hosted service, bug bounty provider, and consortium organizations authorized by the CVE Program to assign [CVE IDs](#) to vulnerabilities and publish [CVE Records](#) within their own specific scopes of coverage.

CNAs [join the program](#) from a variety of business sectors; there are minimal requirements, and there is no monetary fee or contract to sign. View the list of [CNA partners](#).

CNA Program Growth

Currently, there are [525 CNAs](#) (522 CNAs and 3 CNA-LRs) from [43 countries](#) and 1 no country affiliation participating in the CVE Program.

Program Organization

Structure	
Program Relationship With Partners	+
Board	+
Working Groups	+

With ENISA, not Mitre



Dutch Institute for
Vulnerability
Disclosure

[About](#) [Partner Information](#) [Program Organization](#) [Downloads](#) [Resources & Support](#) [Report/Request](#)

[Search tips](#) | [Provide feedback](#)

Notice: Expanded keyword searching of CVE Records ([with limitations](#)) is now available in the search box above. [Learn more here](#).

NOTICE — Due to routine maintenance, this [CVE.ORG website](#) will be **unavailable on June 29, 2026, between 10:30 AM and 11:30 AM EDT**. We apologize for the inconvenience and thank you for your understanding.

Dutch Institute for Vulnerability Disclosure (DIVD)

Steps to Report a Vulnerability or Request a CVE ID

Step 1: Read disclosure policy View Policy	Step 2: Contact Email
---	--

Scope	Vulnerabilities in software discovered by DIVD, and vulnerabilities reported to DIVD for coordinated disclosure, which are not in another CNA's scope.
Program Role	CNA
Root	EU Agency for Cybersecurity (ENISA)
Top-Level Root	MITRE Corporation

Happy Wietse, happy supply chain



Dutch Institute for
Vulnerability
Disclosure

CVE-2024-21876

UNAUTHENTICATED PATH TRAVERSAL VIA URL PARAMETER IN
ENPHASE IQ GATEWAY VERSION < 8.2.4225

CVE	CVE-2024-21876			
Title	Unauthenticated Path Traversal via URL Parameter in Enphase IQ Gateway version < 8.2.4225			
Case	DIVD-2024-00011			
Credits	• Wietse Boonstra of DIVD (finder) • Hidde Smit of DIVD (finder) • Frank Breedijk of DIVD (analyst) • Max van der Horst of DIVD (analyst)			
Affected products	Product	Affected	Unaffected	Unknown
	Enphase IQ Gateway	>= 8.0 to < 8.2.4225 (semver)		
		= 7.x (semver)		
		= 6.x (semver)		
		= 5.x (semver)		
		= 4.x (semver)		
			everything else	

CVSS

Scenario 1 : GENERAL			
Base score	9.3 - CRITICAL		
Attack Vector	NETWORK		
Attack Complexity	LOW		
Attack Requirements	NONE		
Privileges Required	NONE		
Confidentiality Impact			
Vulnerable system	HIGH	Subsequent systems	NONE
Integrity Impact			
Vulnerable system	HIGH	Subsequent systems	NONE

CVE-2024-21876

CVE-2024-21877

CVE-2024-21878

CVE-2024-21879

CVE-2024-21880

CVE-2024-21881



Scale up with Harm & Wilco



Dutch Institute for
Vulnerability
Disclosure



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-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.



Scale up with Hamza, Humza and Alex



Dutch Institute for
Vulnerability
Disclosure

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.

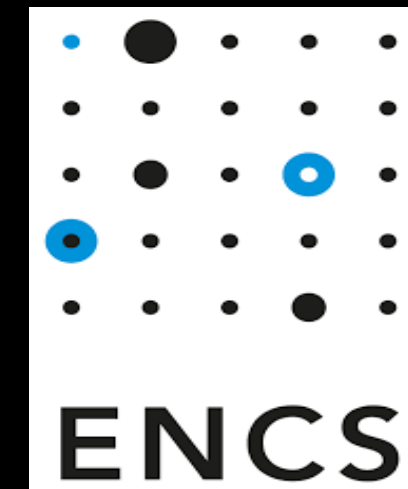


CVE-2025-36756

CVE-2025-36757

CVE-2025-36758

CVE-2025-36759



Harm strikes again...



Dutch Institute for
Vulnerability
Disclosure

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.

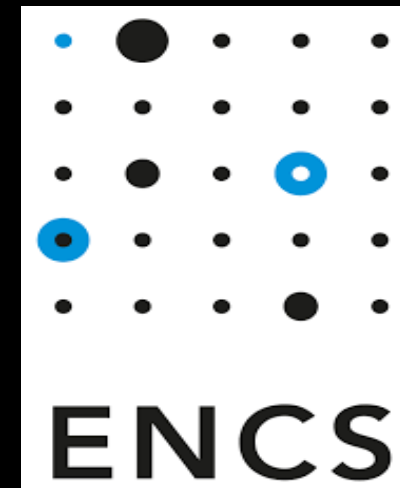
SUNGROW

CVE-2025-36756

CVE-2025-36757

CVE-2025-36758

CVE-2025-36759



Happy hackers, vendors and supply chain



Dutch Institute for
Vulnerability
Disclosure

SUNGROW

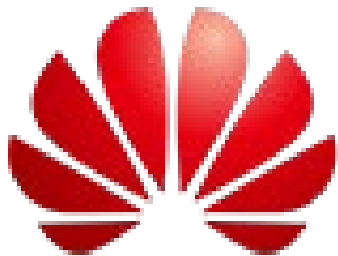
 **MENNEKES**
MY POWER CONNECTION

SOLAX



solar**edge**

GROWATT



HUAWEI



But....



Dutch Institute for
Vulnerability
Disclosure

What if vendors
just don't want to listen
to helpful hackers?

We report to the authorities



Dutch Institute for
Vulnerability
Disclosure



- > RED: Radio Equipment Directive
- > CRA: Cyber Resilience ACT
- > NIS2: Network & Information Systems directive 2

So, how do we get away with all this?



Dutch Institute for
Vulnerability
Disclosure

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.



But we are under attack



Dutch Institute for
Vulnerability
Disclosure

DIVD Dutch Institute for Vulnerability Disclosure
8,122 followers
1w · Edited ·

Security people always say it's not a matter of if, but when you get hacked. It took us (almost) seven years but we can now say that we're the hackers that got hacked. We noticed suspicious activity, investigated, and came to the inevitable conclusion that damn, we got hacked.

So what do hackers do when they get hacked? Handle it the way we think it should be handled. That is open, transparent and honest, even if it sucks. So far, we've been in full incident response mode, blocked access to our infrastructure and started a forensics investigation with the assistance of a third party incident response team.

This is an attack we have not seen before. Not because it's our first, but because the modus operandi indicates that this is an agentic AI powered attack. Careful investigation takes time and our investigation is still ongoing. At this moment we can't rule anything out yet, so we handle this situation as a worst-case-scenario and assume breach until proven otherwise.

Today we have informed the directly involved parties, reported the incident to the Autoriteit Persoonsgegevens and the National Cyber Security Centre and discussed our options with the police.

Our priorities at this point are keeping our infrastructure isolated and secure, focusing on the forensics and looking after our volunteers who have worked for a safe digital society for the past years and in the meantime we learn a lot from this type of attack.

Our next public update follows on Monday 28 September, or sooner if we have more to share.

For questions and press please reach out to [Marieke R.](#) or communications@divd.nl. She is the spokesperson for this incident.

Previously we stated that we handle this situation as a worst case scenario until we can prove otherwise, and that we would be open, transparent and honest, even if it sucks. That's why we think it is only fair to share some of the scenarios we keep in mind. Our worst case scenario is that a still unknown actor targeted DIVD directly and tried to get a hold of our crown jewels.

Another scenario is smash and grab, where an attacker just kicks in the door and takes what they can. Thankfully we have no facts so far that point us to our worst case scenario, which unfortunately doesn't mean we can rule it out yet. We can also state that we see no link to any known public threat actors or involvement by a former volunteer.

By now we have a pretty good idea of how they got in, by exploiting a technical vulnerability. Unfortunately we're not able to share any details, because it could interfere with the ongoing investigation or cause more victims. But what we can say for sure is that it was not Citrix Netscaler. As soon as we can share more, we will scan for & notify other possible victims, like we always do.

The attack itself was loud and very very messy. We could see the agent working automated, because after every action it decided the next step itself, at the speed of light and sloppy logic or pattern. It also looks like the agent skipped a few steps on its learning curve, because it has done some pretty dumb things, like polluting its own MITM attack with password spraying. More on that later. But what makes this attack pretty cool is that the agent is so overexplaining in its comments that it makes our job in reverse engineering a lot easier.

This is everything we can share for now. Thanks to our partners, volunteers and the community for their support, kind messages and confidence. And thanks to [Nationaal Cyber Security Centrum \(NCSC-NL\)](#), [Merlon Security](#), [NVISO Security](#) for the support.

Our next public update follows on Thursday October 1st, or sooner if we have more to share.

For questions and press please reach out to [Marieke R.](#) or communications@divd.nl. She is the spokesperson for this incident.

DIVD Dutch Institute for Vulnerability Disclosure
8,122 followers
6d · Edited ·

When hackers get hacked, we deal with it in hacker style. While trying to figure out how the attackers got into our own systems, **we found two zero-day vulnerabilities in Zammad.**

Used together, they allowed the attackers to hijack sessions, run code remotely and escalate privileges from the Zammad user to root, in seconds, due to the agentic part of this hack. From there they were able to access other services and read and exfiltrate data. We urge everyone using any version of Zammad to update to version 7 or take it offline as soon as possible.

Thanks to proper network segmentation and the actions of our IT and Incident Response Team after detection, we were able to stop the attackers from going deeper into our systems and network. Unfortunately some of the damage was already done. We've found signs of compromise that we're still looking into, and until we can prove otherwise we assume breach. Still, stopping the attackers is a win and in a situation like this you take every win you can get.

Together with [Merlon Security](#) we found two zero-days in [#Zammad](#). On their own they are already significant and combined really nasty. We issued CVE-2026-102489 and CVE-2026-102490, are in touch with Zammad and in the meantime we have started notifying owners of vulnerable instances.

We're still in full investigation mode, and our next public statement will be on October 1st. For more information about the CVEs and a script to check your logs for abuse, check our case file. Link in comments.

TLDR: If you run any version of Zammad, update to version 7 or take it offline as soon as possible.

For questions and press please reach out to [Marieke Rijken](#) or communications@divd.nl. She is the spokesperson for this incident.

DIVD Dutch Institute for Vulnerability Disclosure
8,122 followers
5d · Edited ·

This is probably the most painful and awkward part of being hacked, sharing which data got out. But waiting until you have all the details does not make the world, and digital society, any safer. If it was your ass on the line, you'd want to know, right? We said we would be open, transparent and honest even if it sucks. So here we go.

Through the two zero-days in Zammad, the attackers got in and were able to read and exfiltrate data from other services. We know for sure that user data of our volunteers got out, such as DIVD email addresses and possibly contact details. Whose data and exactly which data is still being investigated, but it does mean it's now easier for someone to pose as a DIVD volunteer.

The full overview of what is compromised and what is not lives in our casefile, <https://lnkd.in/e2w-8sAY> and we update that page whenever we know more.

If you get an email or contact request from someone at DIVD that feels slightly off, check with us first at communications@divd.nl. Our volunteers are our favourite humans in the world and they would never ask you for anything unethical, rude, personal or anything that could harm you. Please be excellent to each other, it has been a tough week for them.

Our next public update follows on Friday 9 October, or sooner if we have more to share.

For questions and press please reach out to [Marieke R.](#) or communications@divd.nl. She is the spokesperson for this incident.

DIVD Dutch Institute for Vulnerability Disclosure
8,122 followers
4d ·

Hooray, we are contained! When we shut down our infrastructure on Tuesday 22nd, we hoped that would do the trick. Now we know for sure it did, so we've officially declared ourselves contained.

That means we can take the pressure off a bit and focus fully on the investigation, figuring out all the details and writing the reports you've all been asking for.

We're also doing a spontaneous talk at the [ONE Conference](#) next Wednesday. You might notice it's a no publicity talk, which might look weird since we've been so transparent about this. We do this on purpose, so we can be even more transparent during the talk. We'll speak to the press afterwards.

Now we're going to catch up on the 4289658 hours of missed sleep, if the 5788 liters of Club-Mate lets us.

Next public update is still planned for Friday October 9, or sooner if we have more to share. For questions and press, please reach out to [Marieke R.](#) or communications@divd.nl. Full details in our casefile, <https://lnkd.in/e2w-8sAY>

UPDATE

Security people always say it's not a matter of if, but when you get hacked
It took us (almost) seven years but we can now say that we are the hackers that got hacked.

UPDATE

We said we'd treat this as a worst case until we can prove otherwise, here is what we know so far

UPDATE

We got hacked through zero-days in Zammad. Update as soon as possible to version 7 to avoid the same.

UPDATE

We said we would be open, transparent and honest, even if it sucks. This is the part where it sucks.

UPDATE

Hooray, we can declare ourself contained!

We are under attack and opened the candy jar



```
[REDACTED]divd.network:/$ cat [AGENT_NAME1].sh
#!/bin/bash
# [AGENT_NAME1].sh : NON-working-hours (16:00-05:00 UTC) L2 MITM harvester scheduler.
# Staggered with [AGENT_NAME2] (working hrs 05:00-16:00): yields when [AGENT_NAME1] is
# active, so the two NEVER poison the same MACs at the same time.
# Poisons same pairs as [AGENT_NAME3].py: .1/.2 <-> .11/.15/.16. Reversible per window.
```

```
[REDACTED].divd.network % cat [REDACTED].py

#!/usr/bin/env python3
# ONE harmless open-relay test: external sender → DIVD's own [REDACTED] inbox (readable via [REDACTED] API).
# Sends exactly one message with a unique marker; no third party, no spam, no phishing.
```



Dutch Institute for
Vulnerability
Disclosure

Help us
to
help you



Dutch Institute for
Vulnerability
Disclosure

Respond to our notifications

partner: chris@divd.nl

divd.nl/donate

7H4NX



Demo time!



Dutch Institute for
Vulnerability
Disclosure

