We got hacked, and your email address leaked, unfortunately

Hi,

We're sorry that your email address was in the data that got stolen from us. When we got hacked, we promised to be open, transparent and honest about it, even if it sucks. So here we go.

We had your email address because you are or were a DIVD volunteer, because we were in touch at some point through csirt@divd.nl or an address ending in @csirt.divd.nl, or because it was part of a set of leaked credentials that came through our CSIRT. In that last case the data only held a partially masked version of your password, never the full one.

Based on the final report of our investigation, which we will publish on Wednesday 25 November at 13:37, we have no reason to assume this leads to a high risk for you. But the attacker has your email address, and we don't know if they have shared it with others or with whom. That means it could be used for spam and phishing, including targeted phishing through social media or messages pretending to come from us.

What data was leaked about you because you have a divd.nl email address

Because you have a divd.nl email address, the attacker may have had access to more data about you.

Name	**Yes, Arthur Dent**
Email	**a.dent@divd.nl**
Did your phone number leak	**No**
Did your Google profile picture leak	**No**
Are you recognizable in your profile picture	**No**

What we've done

Within hours of discovering the attack we isolated our environment to stop the attacker from getting any further, and we reported the incident to the NCSC and the Dutch Data Protection Authority (Autoriteit Persoonsgegevens). From day one we assumed the worst case scenario, that data had leaked, and on 1 October we published an initial page on our website about which data we expected to have leaked, so you may have seen this already. This page has been updated with the final status, which is not as bleak as our worst case scenario. We also filed a police report and are rebuilding all systems in the affected network segment and a few more for good measure.

What you can do

Yet another data leak with your email address in it is the last thing you need, so here are a few tips that might help you out.

- Check what data of yours is known at **haveibeenpwned.com**
- Emails from DIVD always come from an @divd.nl or @csirt.divd.nl address and contain a link to one of our sites
- You can always email **csirt@divd.nl** to validate an email

What happened

On the evening of 21 September, when an administrative account logged into Zammad, the helpdesk system behind our CSIRT mailbox, the attacker used a zero-day vulnerability to take over the administrative session within 1.3 seconds. At 21:27 the attacker gained access to our internal network, and twenty minutes later, by using a second zero-day, they gained full control over the server. After this the attacker used an Agentic Offensive Framework (ARTEX) to attack other systems in our network.

We discovered the attack on 22 September, contained the attack and started a forensic investigation, which is now finished and confirms what data was leaked.

More information

More information can be found on these pages.

- **divd.nl/hacked**
  The update page of this hack, where we'll publish the final report with our security measures and what we did after discovering the incident on 25 November 13:37
- **csirt.divd.nl/cases/DIVD-2026-00014**
  The case file of our hack with all technical details

If you have any questions, you can reach our Data Protection Officer at **dpo@divd.nl**.

On behalf of the DIVD board,
Shairesh Algoe
Chairman