

# DIVD's work is of great importance, here is why

This page explains why our work matters to society, partners, and other organizations.

## DIVD scans the entire internet

Traditional methods, like penetration tests, often focus on a specific scope, usually limited to an organization's IP addresses or URLs. In contrast, DIVD seeks to identify all systems with a particular vulnerability, often discovering issues in systems that organizations were unaware they had.

### DIVD takes this a step further.

Because we work for the common good and adhere to guidelines for ethical hacking, we extend our reach beyond the limits imposed on governments or commercial security companies. This allows us to determine with greater certainty whether a system is vulnerable. An email notification from DIVD always indicates a vulnerability that needs immediate attention.

### DIVD scans for both regular security vulnerabilities and zero-day vulnerabilities.

DIVD independently assigns new unique identifiers (CVEs) when new (previously unknown) vulnerabilities are identified by its researchers.

### DIVD is known for its transparency & collaboration.

DIVD is recognized for its transparent approach in reporting vulnerabilities and the actions taken to resolve them. This level of openness fosters trust within both the cybersecurity community and the general public. We promote ethical hacking and responsible disclosure while striving to tackle broader cybersecurity challenges. Unlike many cybersecurity organizations, DIVD is a non-profit entity, run by volunteers.

### DIVD actively engages with the cybersecurity community, including researchers, ethical hackers, and other stakeholders, to share knowledge and improve collective security efforts.

## What happens when we find a vulnerability? Here's an example.

A good example of what the world would look like without DIVD's efforts is [the SolarMan case](#). In 2022, a DIVD researcher found a GitHub repository containing the username and password for SolarMan's Super Admin account. These credentials were visible to anyone who would visit the GitHub page, meaning that anyone in the world with internet access could have gained unauthorized access to nearly 1,000,000 installations.



### SolarMan's Password Oopsie

The 1,000,000 installations refer to solar power plants (installations) managed through the SolarMan platform. These installations have a total power output of over 10GwP (gigawatts peak). Most of these systems are located in China and Australia, with a significant number of over 40,000 in The Netherlands.

DIVD contacted the company responsible for the repository. Eventually, the exposed password was reset and the repository was deleted. But what if the vulnerability hadn't been discovered and the credentials remained publicly available?

Cybercriminals could theoretically have been able to gain access to the SolarMan Super Admin account, potentially controlling nearly 1,000,000 installations. They could theoretically have had the ability to alter system settings, disrupt services, or disable installations, causing widespread operational issues.

Sensitive information could potentially have been exposed, leading to data breaches. Compromised systems could theoretically have been used to deploy malware, resulting in further security incidents and potential damage to connected networks.

### The company's reputation could have been severely damaged, resulting in a loss of trust from customers and partners.


Note that it is very complex to summarize any DIVD case, or make accurate and precise assumptions about which risks were specifically mitigated. If you have any questions, please read about our case on the CSIRT

## Suggested Articles

**CULTURE**

**Our yearly get-together was a great succes!**


Lorem ipsum dolor sit amet consectetur. Ultricies faucibus sit ante vestibulum dictum venenatis commodo.



**CULTURE**

**Microsoft update makes Outlook very vulnerable**

Lorem ipsum dolor sit amet consectetur. Ultricies faucibus sit ante vestibulum dictum venenatis commodo.



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.

#### ABOUT

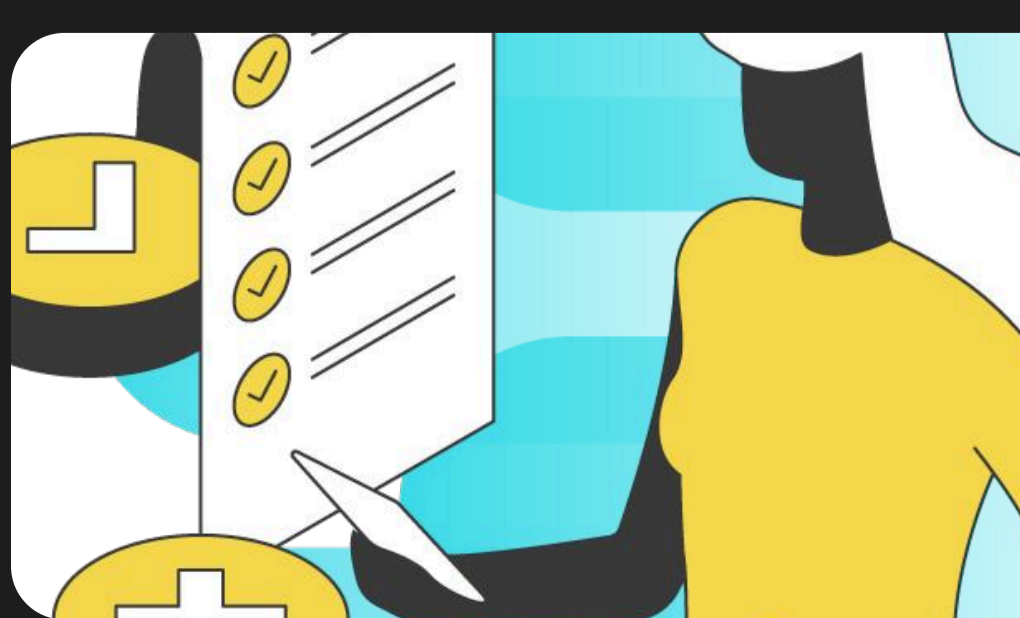
[Who we are](#)  
[What we do](#)  
[The Team](#)

#### SECURITY

[Code of conduct](#)  
[Security Policy](#)  
[ANBI](#)

#### STAY UP TO DATE

[Newsroom](#)  
[Twitter](#)  
[Github](#)  
[Contact](#)

### 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.