

My CERT PL

**Free security tools for everyone in Poland:
an update**

78th TF-CSIRT meeting, Stockholm

Krzysztof Zajac

CERT PL

Quick recap: moje.cert.pl a year ago

- Anyone can join.
- Possibility to add any number of domains and subnets.
- Features:
 - 1.scan results,
 - 2.password leaks,
 - 3.network events,
 - 4.security advisories,
 - 5.Warning List check.

Security scanning

- A couple dozen modules detecting various problems (from low-severity, such as misconfigured SSL, to SQLi or RCE).
- What changed since 2025: we decreased the scan time and added more modules.

Tool: **Artemis**: <https://github.com/CERT-Polska/Artemis>, uses other open-source tools under the hood: **Nuclei**, **SQLmap**.

Severity	Resource	Time	Vulnerability/Misconfiguration	Vulnerability type
High	example.com:443	2026-06-03 12:10:55	The following URLs contain versions of WordPress that are no longer supported and are marked as insecure in the version list at https://api.wordpress.org/core/stable-check/1.0/ : https://example.com:443 - WordPress 6.3.3 If the site is no longer in use, we recommend disabling it to eliminate the risk of attack via known vulnerabilities in older versions of WordPress. If it is still in use, we recommend using the automatic updating mechanism for WordPress and plugins.	insecure/unsupported version of WordPress
Medium	example.com	2026-06-03 12:10:55	The following domains do not have email sender verification mechanisms configured correctly: Error: example.com: No valid DMARC record found. We recommend using all three mechanisms: SPF, DKIM, and DMARC to reduce the chance that a spoofed message will be accepted by the recipient's server. Implementing these mechanisms will significantly increase the chance that the recipient's server will reject spoofed email from the above domains. You can verify the correct implementation of email sender verification mechanisms in your domain at https://bezpiecznapoczta.cert.pl	incorrect configuration of SPF/DMARC mechanisms

Password leaks

- Types: stealer logs, leaked website database dumps, combolists, ...
- Data sources:
 - Commercial providers.
 - Public data.
 - Own hunting.
 - **Data from sectoral CSIRTs.**

example.com

Password leaks of people using the website

Password leaks of users logging in to websites on this domain. For example, a user (using a username or email address on any domain, not just `example.com`) logging in to a service on the `example.com` domain.

Show

10

 position

Search:

▼ Date of acquisition	▼ Date of publication	Description	▼ Account ⓘ	Fragment of the entry	▼ Login page ⓘ
2026-06-03	2026-05-24	Data stolen using malware...	admin	Unknown	https://example.com

Items 1 to 1 of 1 total

«

◀

1

▶

»

Domain account data leaks

Password leaks of users with email addresses in this domain. For example, a user in this domain `nowak@example.com` logging in to services on any domain (both in `example.com` and external domains, e.g. `example.com`).

Network events

- Malware infections.
- Hosts that perform scanning.
- Servers that host phishing.

And many more. Tool: **n6**: <https://github.com/CERT-Polska/n6>

More than 90 data sources, e.g. **Shadowserver**.

Address

Filter by specific address

✕ Clear filters

Show 10 position

Search:

	Time of event occurrence	Address	Category	Event name	Confidence
▼Details	2026-05-16 10:05:06	198.51.100.1	bots ⓘ	smokeloader ⓘ	Medium

Details of the incident:

This device has been infected and is part of a botnet. This means that it can be used by an attacker to perform malicious activities. This information should be verified and actions taken to resolve the situation. Detected botnet family name: smokeloader

Items 1 to 1 of 1 total

Warning List check

- 141 million page views blocked in 2025.
- Phishing, scams, etc.
- No actions needed from users, the block happens on DNS level.
- Supported by most major Polish ISPs.
- We can block a site in as fast as **5 minutes**.
- **In moje.cert.pl a user can check whether their network is protected.**

Security advisories

- For non-technical users.
- For administrators.
- Multiple channels: e-mail (without registration), RSS, API, ...
- New since 2025: **easy subscription without an account.**

For administrators

Critical vulnerability in Authentik software

The CERT Polska team informs about a critical vulnerability in the Authentik software and recommends immediate update.

03-06-2026

[86/2026]

For users

The link to "verify" your account may lead to loss of login details

 We're seeing a campaign impersonating an email service provider. The message contains information about a supposedly planned account deactivation or deactivation.

02-06-2026

[85/2026]

For users

A "Payment Confirmation" may contain more than just a document

We're observing a campaign using the image of Alior Bank. The emails send recipients information about a supposed payment confirmation regarding a document sent by the customer.

01-06-2026

[84/2026]

What is new since 2025?

Organization infrastructure/asset inventory

- Data collected during security scanning.
- Gathered information:
 - Domains, subdomains, IPs and ports.
 - Exposed login panels and VPN gateways.
 - CMS and CMS plugins.
 - Other technologies.

What incidents can we prevent?

Infrastructure



High-risk
vulnerabilities

2

[Check](#)



Hosts found

11



Open
ports

22



Found technologies

6

[Manage](#)



More
statistics

[Check](#)

Filters

Active filters: 0

Expand all

Collapse all

Sort by:

First seen (descending)



Host

✓ 198.51.100.3

Found during scan: vpn.example.com,
vpn.other-domain.example

IP address

198.51.100.3

Ports

22, 80

Vulnerabilities

—

Network events

—

Update time

First: June 3, 2026 12:05 PM

Last Posted: June 3, 2026 12:05 PM

Host

✓ 198.51.100.2

Found during scan: api.example.com,
api.other-domain.example,
demo.example.com, demo.other-
domain.example, example.com

IP address

198.51.100.2

Ports

22, 80

Vulnerabilities

—

Network events

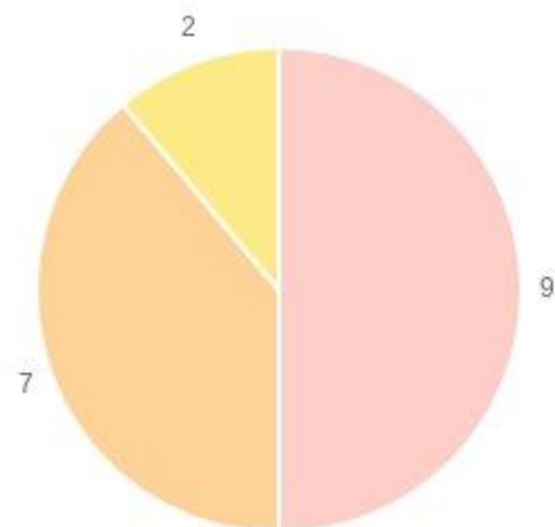
—

Update time

First: June 3, 2026 12:05 PM

Last Posted: June 3, 2026 12:05 PM

Technologies



Items 1 to 3 of 3 total

Technology

Number

Nginx

9

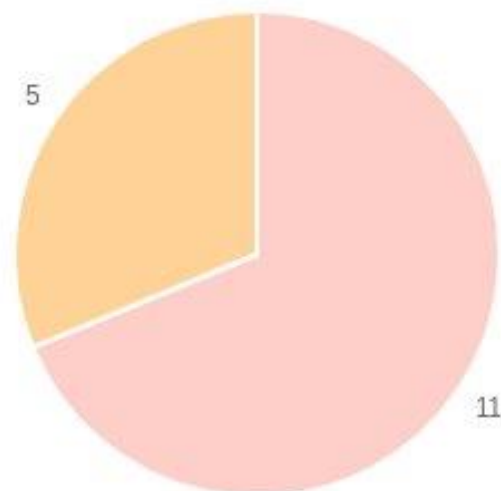
PHP

7

Python

2

Services



Items 1 to 2 of 2 total

Protocol

Number

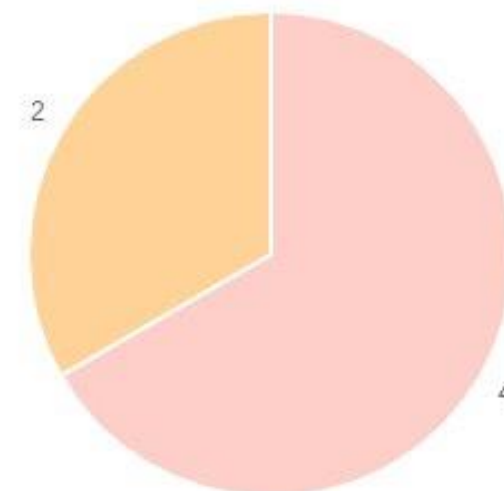
http

11

ssh

5

Publicly accessible login panels



Items 1 to 2 of 2 total

Publicly accessible panel

Number

wordpress-login

4

phpmyadmin-panel

2

Features

- Filtering by technology, port number, protocol, ...
- Showing newly added hosts.
- Vulnerabilities in technologies on a particular host.
- Soon: e-mail notifications.
- Example of a large telecom.

Vulnerabilities in your infrastructure

- Infrastructure data collected during scanning.
- Two vulnerability data sources:
 1. vulnerability.circl.lu
 2. nvd.nist.gov
- Why two data sources?
- Using a LLM to translate vulnerability information.
- Heuristics on what to notify about: CVSS + EPSS + KEV.
- Heuristics on whether a CVE matches a product: CPE is not enough.

Vulnerabilities in your infrastructure

[Organizations](#) / [Example institution](#) / Vulnerabilities in technologies in use

Vulnerabilities in technologies in use

We identified the technologies used in your organization. Based on publicly available external sources, we checked whether this software has any known security vulnerabilities. **Make sure your version and configuration are secure!**

You will also receive information about new vulnerabilities by email.

Filters

Active filters: 1

Search:

Vulnerability ID (CVE)

Description

Severity

Affected versions

Publication date

CVE-2026-17544

Passing specially crafted data to the bccomp() function may result in memory corruption, allowing an attacker to take control of the server or cause the PHP application to crash.

view source

high

CVSS: 9.8

EPSS: 0.00

PHP

8.4.* to below 8.4.24

8.5.* to below 8.5.9

2026-07-30

CVE-2026-17543

Incorrect processing of backslash characters in parameters supplied by an attacker enables an SQL injection attack, allowing unauthorized access to and modification of database data.

view source

high

CVSS: 9.8

EPSS: 0.00

PHP

8.2.* to below 8.2.33

8.3.* to below 8.3.33

+ 2 more

2026-07-30

Implementing v1 was 30% of the work

After implementing the first draft we learnt that:

- Some CVEs don't have CPEs (e.g. `cpe:2.3:a:apache:http_server:2.4.54:*:*:*:*:*:*:*`), so we always need to match by product name.
- There are multiple products with same name (e.g. multiple projects named Sentry).
- Some CVEs have & in the description and they're not vulnerabilities in Accelerated Mobile Pages.
- CVSS is sometimes greatly exaggerated.

Implementing v1 was 30% of the work

After implementing the first draft we learnt that:

- We needed multiple LLM prompt iterations before the translations were acceptable.
- Even if a technology is mentioned (e.g. Cloudflare), the vulnerability may not be related (*to secure your installation, enable reverse proxy such as Cloudflare*).
- Besides heuristics, we decided to use a LLM to match CVEs with products.
- **Monitoring is crucial, human-in-the-loop is worth considering.**

Features for sector CSIRTs

Features:

- Statistics.
- Reports.
- API.
- Easy contact with entities.

Hot topic because of NIS2 implementation!

Features for sector CSIRTs

CSIRT Dashboard

Sample Sector CSIRT (Sample Sector)

Data scope

All data

Date range:

30.08.2026 - 28.09.2026

Print

!

High-risk vulnerabilities

+349 compared with the previous period

519

@

New entities

+3 compared with the previous period

3

🔑

Password leaks

-484 compared with the previous period

1155

📶

Network events from the n6 system

+0 compared with the previous period

0

Password leaks

Top 10 organizations

Name	Count
Sample organization 1	594
Sample organization 2	341
Sample organization 0	220

View all

Password leaks in organizations under your jurisdiction

total=1155

594

341

220

Sample subsector 0 in Sample sector

Sample subsector 1 in Sample sector

Sample subsector 2 in Sample sector

Full report

Why set up such initiative in your country?

Every country needs:

1. Security services for entities that don't have significant security budget.
2. A way to share information&advisories without being dependent on bigtechs.
3. Features that **prepare for the incoming CVE deluge**:
 - advisory sharing,
 - a way to quickly warn everyone with a Fortinet or Gitlab about a CVE,
 - periodic security scanning.

How to set up such initiative in your country?

Advice from 2025:

- Be agile: don't plan too much.
- Start small: don't have network events for now? Start without them!

Advice for now:

- After a successful launch it's time to secure the project:
 - tests,
 - bus factor protection,
 - balance between implementing new features and stability,
 - More serious engineering for bigger complexity.

Project management workflow should differ depending on the lifecycle.
(advice that always holds: choose boring technology).

Statistics

- More than 23k users (**2x growth** since last presentation).
- More than 27k domains (**2x growth** since last presentation).
- More than 900k vulnerabilities and misconfigurations found (**~4x growth** since last presentation), including 67k high-severity.
- 10k advisory subscribers.
- Including scanning of public entities in Poland: almost 1.9M vulnerabilities and misconfigurations found.
- What is the status of the scan time?

Plans

- A feature for users to check whether a file is malicious without sharing it (as is the case of e.g. VirusTotal).
- Onboarding more sectoral CSIRTs (at this moment, **three** use the service: the CSIRTs for the banking, health and infrastructure sectors).

Thank you!

Any questions?