National Cyber and Information Security Agency

NÚKIB

BRNO • FEBRUARY 10, 2025

# COORDINATED VULNERABILITY DISCLOSURE IN THE CZECH REPUBLIC

twopager

- **The National Cyber and Information Security Agency (NÚKIB) is finalizing the development of a national Coordinated Vulnerability Disclosure (CVD) policy. This initiative aims to promote CVD as an effective tool for strengthening cybersecurity while outlining its strategic vision.**
- **In addition to publishing the national CVD policy, NÚKIB plans to launch a web platform that will provide easy and comprehensible access to CVD-related information. This platform will include, for example, a sample CVD policy for public and private organizations, along with other useful resources.**
- **The National CVD policy is set to be published during the 1st-2nd Quarter 2025.**
- **Based on the requirements of NIS2[1], CVD is mentioned in the new draft law on cybersecurity, in which:**
  - **the governmental CERT as a part of NÚKIB is designated as the coordinator for the purposes of CVD (Article 12 paragraph 1 NIS2),**
  - **everyone has the possibility to report vulnerabilities to the coordinator, even anonymously (Article 12 paragraph 1 NIS2).**
- **NÚKIB is assessing the feasibility of implementing its own CVD policy, which would cover vulnerabilities in the agency's exposed assets, such as web applications, to enhance cybersecurity resilience.**

**DISCLAIMER: This document provides an overview of the CVD landscape in the Czech Republic. The timeline and final form of the outlined CVD initiatives are subject to change and may differ from those presented in this Two-Pager.**

## What is CVD?

CVD is a structured process that enables vulnerability researchers to collaborate with relevant stakeholders, such as vendors and ICT infrastructure owners, to address security risks effectively.

The process ensures that reported vulnerabilities are disclosed only after a fix, patch, or mitigation has been developed, minimizing potential threats. This approach promotes responsible reporting, enhances cybersecurity resilience, and allows stakeholders to mitigate risks before vulnerabilities can be exploited.

## NÚKIB Goals for CVD

NÚKIB recognizes CVD as a key mechanism for strengthening the security of ICT products. The NIS2 Directive also underscores the importance of CVD, placing specific obligations on EU Member States.

In response, NÚKIB aims to:

[1] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Full text here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555.

a) **Develop a national CVD policy** to provide a strategic framework for vulnerability disclosure.

b) **Designate one of its CSIRTs as the national CVD coordinator** to facilitate efficient collaboration.

c) **Implement CVD within NÚKIB's own systems**, including web applications, to lead by example.

## What is the National CVD policy?

The National CVD Policy provides a comprehensive framework for CVD, outlining its role within the legal system of the Czech Republic. Its goal is to promote CVD as a key mechanism for enhancing the security and resilience of ICT infrastructure.

To support this effort, NÚKIB plans to develop a web-based CVD platform, enabling both public and private organizations to adopt CVD practices seamlessly.

## What is the Role of a CVD Coordinator?

The CVD coordinator plays a crucial role in managing the disclosure process by:

- Identifying and contacting stakeholders affected by a vulnerability.
- Assisting reporters in handling disclosures.
- Negotiating disclosure timelines and coordinating responses to vulnerabilities impacting multiple entities.
- Informing other national coordinators about vulnerabilities with cross-border implications.

The draft of the new Czech Cybersecurity Act[2] designates the Governmental CERT, part of NÚKIB, as the national CVD coordinator. Under this framework, any legal or natural person will have the right to report vulnerabilities to the coordinator.

## Legal Aspects of CVD

There are several legal aspects that need to be addressed regarding CVD. The most significant is criminal law, as unauthorized hacking is a criminal offense in the Czech Republic, regardless of the hacker's intent. However, according to the Criminal Code of the Czech Republic, this can be mitigated if the ICT product owner grants explicit consent for security testing.

Another key legal area impacting CVD policy development is personal data protection, primarily governed in the EU by the GDPR[3]. The strict requirements for handling personal data in tested ICT products, including potential obligations to establish data processing agreements between researchers and data controllers, could pose challenges to the practical implementation of CVD.

NÚKIB has consulted the legal aspects with relevant authorities and has been exploring ways to address these challenges in the National CVD Policy to ensure compliance with legislative requirements while maintaining the functionality and efficiency of the CVD process.

[2] The information on the new Act on Cyber Security is available here: https://osveta.nukib.gov.cz/course/view.php?id=168.
[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Full text here: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32016R0679

National Cyber and Information Security Agency

NÚKIB

## INFORMATION SHARING: TRAFFIC LIGHT PROTOCOL

Conditions for information sharing are guided by Traffic Light Protocol (available at https://www.first.org/tlp/).

| Color | Condition |
|---|---|
| TLP:RED | For the eyes and ears of individual recipients only, no further disclosure. Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. |
| TLP:AMBER | Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. |
| TLP:AMBER+STRICT | Restricts sharing to the organisation only. |
| TLP:GREEN | Limited disclosure, recipients can spread this within their community. Sources may use TLP:GREEN when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. Note: when “community” is not defined, assume the cybersecurity/defense community. |
| TLP:CLEAR | Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction. |