**REPUBLIC OF ALBANIA**
**NATIONAL CYBER SECURITY AUTHORITY**

No. 2866 Prot. Tirana on 03.11.2025

# ORDER

**No. 317 date 03 / 11 / 2025**

## ON THE APPROVAL OF THE POLICY ON COORDINATED VULNERABILITY DISCLOSURE

In accordance with law no. 25/2024 "On cyber security",

**I ORDER:**

1. Approval of the policy "On coordinated vulnerability disclosure", according to the text attached to this order and forming an integral part thereof.
2. The National Cyber Security Authority shall be charged with the implementation of this order.
3. This order shall enter into force immediately.

**DIRECTOR GENERAL**

**IGLI TAFA**

# COORDINATED VULNERABILITY DISCLOSURE (CVD) POLICY

## 1. Introduction

Identification and exploitation of vulnerabilities are often used to compromise the information and security of affected information systems and networks. These vulnerabilities can be used in committing cybercrime, economic crimes, theft of information or credentials, and in some cases have also been linked to attacks on strategic infrastructures in certain countries. For this reason, it is important to implement policies for the reporting and handling of vulnerabilities.

This policy establishes a framework for the coordinated reporting and disclosure of identified vulnerabilities in affected ICT products and services, ensuring compliance with Law No. 25/2024 "Për sigurinë kibernetike" as well as based on international best practices.

The National Cyber Security Authority (AKSK), in its capacity as coordinator for vulnerability detection, is responsible for the implementation of this policy for the purpose of identifying and addressing vulnerabilities to strengthen cyber security at the national level.

For the implementation of this policy, AKSK collaborates with natural and legal persons who report vulnerabilities, such as operators of critical and important information infrastructures, security researchers, manufacturers, vendors, as well as other interested entities, to address the discovered vulnerabilities and protect the entities or products where they are identified.

AKSK coordinates the identification and documentation of vulnerabilities in the vulnerability register. The Authority, in implementation of law no. 25/2024 "Për sigurinë kibernetike", identifies, analyses and provides assistance to operators of critical and important information infrastructures in the event of a vulnerability identified mainly or reported by operators of information infrastructures. Furthermore, The Authority will also assist in addressing vulnerabilities identified in other entities, reported by natural or legal persons.

## 2. Scope of application

This policy applies to vulnerabilities as follows:

- Vulnerabilities in applications, software, and systems;
- Vulnerabilities in devices, hardware, and integrated systems;
- Vulnerabilities in networks and information systems, including critical and important information infrastructures, as well as governmental and independent institutions in the Republic of Albania.
- Vulnerabilities reported by other natural or legal persons.

## 3. Definition of vulnerability and incidents related to it

### What is a vulnerability?

Vulnerability is a weakness, sensitivity, or flaw in ICT products or services, which can be exploited by a cyber threat. A vulnerability may lead to an event that compromises the security of a device, operating system, application, protocol, network or information system.

### A vulnerability is distinguished from a cybersecurity incident

A vulnerability is different from a cybersecurity incident, which is an event that has a real or potentially negative effect on the security or performance of a system. A cybersecurity incident is any event that compromises the availability, authenticity, integrity, confidentiality of data stored, transmitted or processed, or of services provided or accessible through information networks and systems. Incidents may arise as a result of exploiting a vulnerability, but they are treated separately and in accordance with the respective procedures.

**Examples of cybersecurity incidents related to vulnerabilities include the following:**

- **Attempted intervention:**
  - Exploitation of known vulnerabilities: attempts to compromise a system or disrupt a service by exploiting vulnerabilities (*buffer overflow, XSS, backdoor*, etc.).
  - Multiple attempts to access with credential breaches (*brutte force*, password breaking...).
  - Unknown attack using an exploit.

- **Intervention:**
  - Application compromise: is carried out by exploiting software vulnerabilities.

- **Denial of making available on the market:**
  - DoS/DdoS refers to a cyber incident where many devices distributed across the internet send a large amount of traffic towards a service, application, website or server, with the aim to overload him, to slow down the functioning or to make it unavailable the service for users by interrupting it.

- **Vulnerable services and systems:**
  - Publicly accessible services that may have weak cryptography (web servers vulnerable to POODLE/FREAK attacks, Heartbleed, FREAK...).
  - DDoS amplifier: publicly accessible services that can be used for reflection or amplification of DDoS attacks, for example, by exploiting the functionality of an open DNS server that converts domain names into IP addresses to overload a specific network or server with an amplified amount of traffic.

- System vulnerable for various reasons (poor proxy configuration on a Web Proxy Autodiscovery Protocol client, outdated system, lack of antivirus and/or firewall, etc.).

**4. The Authority's competences in the identification of vulnerabilities**

The National Cyber Security Authority, pursuant to Article 9 and Article 14 of Law No. 25/2024 "Për sigurinë kibernetike", acting as the National CSIRT, in the capacity of coordinator for vulnerability detection, performs the following duties:

a) identifies and contacts interested parties;

b) assists natural or legal persons who report a vulnerability;

c) negotiates the timeframes for the discovery and management of vulnerabilities affecting multiple entities.

The National CSIRT, in its capacity as coordinator for vulnerability detection, ensures that appropriate actions are taken by information infrastructure operators regarding the reported vulnerability and guarantees the anonymity of the operator reporting this vulnerability.

When a reported vulnerability affects the information infrastructures of other countries, the National CSIRT, when necessary, cooperates with the CSIRTs of other countries designated as coordinators on the basis of an agreement concluded between the parties.

The National CSIRT develops and maintains a register of identified vulnerabilities, which contains the following data:

a) information describing the vulnerability;

b) the affected ICT products or ICT services and the level of vulnerability in relation to the circumstances in which it may be exploited;

c) guidelines regarding the solutions provided for mitigating risks arising from the identified vulnerabilities.

Furthermore, the Authority, pursuant to Article 30 of Law No. 25/2024 "Për sigurinë kibernetike", is responsible for scans of the networks and systems of operators of critical and important information infrastructures. for the purpose of controlling security measures related to possible vulnerabilities, in any case, by informing the information infrastructure operator in advance, ensuring transparency of the process and guaranteeing the confidentiality of information.

The Authority provides support to natural and legal persons who wish to submit information by reporting a vulnerability they have discovered and acts by anonymizing the data of the

reporter, unless the reporter states otherwise at any time during the management of the vulnerability.

**5. Actions not permitted in vulnerability research**

During the process of searching to identify possible vulnerabilities, it is necessary to act in accordance with the applicable legislation. Reporting a vulnerability to the Authority does not exempt the reporter from the obligation to continue acting in accordance with the applicable legislation following the reporting of this vulnerability. Furthermore, searching for vulnerabilities cannot be used as a pretext to attack a system or any other target.

Actions that are not permitted include the following:
-the use of social engineering;
-compromising a system and maintaining continuous access;
-manipulation of accessed data through exploitation of vulnerabilities;
-use of malicious programs;
-the use of vulnerabilities for any purpose beyond verifying their existence. To demonstrate the existence of a vulnerability, non-aggressive methods may be used, for example by listing a system directory;
-use of *brutte force* to gain access to systems;
-sharing of vulnerabilities with third parties;
-the carrying out of DoS or DDoS attacks.

All research activities for the identification of vulnerabilities must be in accordance with the applicable legislation and the rules set forth in this policy.

All vulnerabilities must be reported immediately to the National Cyber Security Authority as soon as they are discovered and must not be exploited in any way.

It is prohibited for the identified and reported vulnerability to the Authority to be disclosed to the public by the reporter or other persons, before this vulnerability is addressed by the responsible entities and before the Authority makes the decision that publishing the vulnerability no longer poses a risk for its potential exploitation for malicious purposes.

**6. Reporting a vulnerability**

Vulnerabilities are reported to AKSK through communication channels as follows:

- info@aksk.gov.al electronic mail, email;
- telephone: 04 2221 039.

Operators of critical and important information infrastructures may also report identified vulnerabilities through the Incident Reporting Management System, if there have been attempts to exploit the vulnerability.

It is recommended that the information contained in the report be encrypted with the public key linked to this email. The public key for use can be downloaded here: https://aksk.gov.al/link-celes-publik/ .

Reports may concern vulnerabilities in applications and software, devices, hardware or integrated systems, as well as information systems and networks, including government systems and critical and important information infrastructures.

### 6.1 Information required for reporting

To report a vulnerability, the following information is required:
• clear and detailed description of the vulnerability;
• clear and detailed information on how the vulnerability was discovered.
Other information that may be useful during the reporting of the vulnerability includes the following:
• clear evidence of the existence of the vulnerability through screenshots, links, etc.);
• when the vulnerability was discovered;
• any information deemed necessary to locate and resolve the vulnerability as quickly and efficiently as possible.

Upon receipt of the reporting and relevant information, AKSK will confirm its receipt and may request clarification and further information if necessary for the purpose of addressing the vulnerability. AKSK will immediately begin communication with the interested parties for addressing the vulnerability. If the vulnerability involves an operator of critical or important information infrastructure, the specialized technical teams of the Authority provide support to mitigate the impact and remediate the vulnerability as quickly as possible.

### 6.2 Assessment and resolution of vulnerability

When AKSK receives a report about a vulnerability, the first step is to verify whether the reported vulnerability is a new vulnerability in a system, information network, or product, or if it is an end user incident.

In the event that a new vulnerability is identified, the Authority's team manages it by coordinating communication between the reporter and the owner of the affected product, system, or network. After the vulnerability is resolved, the Authority documents it as a new vulnerability in the vulnerability register and coordinates the public disclosure of the vulnerability by anonymizing sensitive information.

In the case of an end user incident, the incident management team of the Authority will perform the assessment and prioritization (*triage*) as well as the classification of the incident, by notifying affected users and interested parties and sharing details and technical solutions, respecting the anonymity of the reporter.

### 6.3 Detection of vulnerability to the public

The disclosure of the vulnerability to the public takes place only after the impact has been mitigated and the vulnerability resolved, in coordination with the reporter and affected parties, and only after the Authority decides that publishing the vulnerability no longer poses a risk for its possible exploitation for malicious purposes. The disclosure of the vulnerability, by anonymising sensitive information, is made on the official website and the social networks of the Authority and is recorded in the vulnerability register.

## 7. Preparedness, Support, and Communication

The National CSIRT is on standby for response and reaction to incidents and vulnerabilities 24/7, providing support for the timely handling and resolution of reported vulnerabilities.

For vulnerabilities related to operators of critical and important information infrastructure, communication with AKSK for reporting and resolving vulnerabilities is carried out through dedicated contact points to ensure rapid communication and support for mitigating the impact, addressing, and resolving them.