CSIRT description for

CESNET-CERTS

the CESNET, a.l.e. security team

1 Document Information

This document is intended to describe the CESNET-CERTS team as required by RFC 2350. It outlines general information about the team, contact methods, its constituency, responsibilities, and the services provided.

1.1 Date of Last Update

This is version 1.5, last updated on 2025-08-15.

1.2 Distribution List for Notifications

There is currently no distribution list for notifications about updates to this document.

1.3 Locations where this Document May Be Found

The current version of this document is always available at https://csirt.cesnet.cz/.

2 Contact Information

2.1 Name of the Team

CESNET-CERTS

2.2 Address

CESNET, a.l.e.

CESNET-CERTS

Generála Píky 430/26

Prague 6

16000

Czech Republic

2.3 Time Zone

Central European Time (CET, UTC+01:00 in winter; CEST, UTC+02:00 in summer).

2.4 Telephone Number

Phone: +420 234 680 222

Mobile: +420 602 252 531

2.5 Facsimile Number

None.

2.6 Other Telecommunication

None.

2.7 Electronic Mail Address

Please send incident reports to *abuse@cesnet.cz*. For other matters related to the team, please use *certs@cesnet.cz*.

2.8 Public Keys and Encryption Information

CESNET-CERTS team uses PGP for secure communication. The CESNET-CERTS team has its own PGP key and each team member also uses an individual PGP key.

CESNET-CERTS team PGP keys:

Master key (used to verify our PGP keys):
User ID: CESNET-CERTS <certs@cesnet.cz>, <abuse@cesnet.cz>
Key ID: 0x97D157FF6F7F277E
Fingerprint: 95FD F42E AC0E A05A 9F4E 0CE1 97D1 57FF 6F7F 277E

Communication key (used for e-mail signing and encryption):
User ID: CESNET-CERTS Operator <certs@cesnet.cz>, <abuse@cesnet.cz>
Key ID: 0xFC3F62D9F458694E
Fingerprint: 87D3 58CA 1C39 F232 1EFF BC58 FC3F 62D9 F458 694E

PGP keys of team representatives:

User ID: Andrea Kropacova <andrea@cesnet.cz>, <ak@cesnet.cz>, <andrea.kropacova@cesnet.cz>
Key ID: 0xE190325902532517
Fingerprint: 23A7 109F 119F 40E6 FBC5 F4F6 E190 3259 0253 2517

User ID: Pavel Kácha <ph@cesnet.cz>
Key ID: 0xDCECE39C9803CB04
Fingerprint: 82E9 A3B1 4487 C25B 5C6A CFA2 DCEC E39C 9803 CB04

All listed keys and their signatures are available from public key servers.

2.9 Other Information

General information about CESNET-CERTS is available at: http://csirt.cesnet.cz/.

CESNET-CERTS also posts updates and announcements on Mastodon: @cesnet_certs.

2.10 Points of Customer Contact

The preferred method for contacting CESNET-CERTS team is via e-mail:

- *abuse@cesnet.cz* (for incident reports)
- *certs@cesnet.cz* (for other matters)

All e-mails are handled by the currently assigned operator – a member of the CESNET-CERTS. During normal working hours (Monday–Friday, 09:00–17:00, see Section 2.3 for time zone), we aim to respond to all e-mails within one business day. Messages that are received outside working hours will be processed on the next working day. For sensitive information, please use PGP encryption when contacting us via e-mail.

For urgent matters requiring immediate attention, you may call the phone number listed in Section 2.4 at any time — this number is monitored 24/7 by the CESNET permanent service desk.

3 Charter

3.1 Mission Statement

CESNET-CERTS is the CSIRT team of CESNET, Association of Legal Entities, the National Research and Educational Network of the Czech Republic.

Main tasks of the team are:

- To serve as a primary Point of Contact for the CESNET network in the field of cybersecurity.
- To maintain international relations with the global CERT/CSIRT community and supporting organizations.
- To cooperate with various national stakeholders including ISPs, content providers, banks, security forces and organizations, academic institutions, public authorities and others.
- To provide security services such as:
  - incident handling and coordination,
  - proactive security services,
  - security education and training.

The team adheres to CESNET's Code of Ethics, which governs professional conduct and information handling.

3.2 Constituency

CESNET-CERTS is the CSIRT team of CESNET, Association of Legal Entities, the National Research and Educational Network of the Czech Republic. Its constituency includes the entire CESNET e-Infrastructure network, specifically all IP address space within Autonomous System (AS) 2852. The team is fully responsible for handling and responding to security incidents related to:

- domains listed at https://csirt.cesnet.cz/en/domains
- the CESNET e-Infrastructure marked as INFRA-AW in the RIPE database

CESNET-CERTS also supports the coordination and resolution of security issues across the entire CESNET e-Infrastructure network as well as in AS48091.

3.3 Sponsorship and/or Affiliation

CESNET-CERTS is a team established by CESNET, Association of Legal Entities. CESNET operates and develops the national e-Infrastructure for science, research, and education, which includes a computer network, computational grids, data storage, and a collaborative environment. It provides a wide range of services to its connected organizations.

3.4 Authority

CESNET-CERTS was established by CESNET, Association of Legal Entities, and operates with authority delegated by CESNET.

All members of CESNET-CERTS are employees of CESNET, Association of Legal Entities.

4 Policies

4.1 Types of Incidents and Level of Support

CESNET-CERTS provides incident handling service for all IP address ranges within AS2852 and AS48091.

The level of support depends on the type and severity of the incident, type of constituent, and the current availability of CESNET-CERTS resources. In all cases, CESNET-CERTS guarantees to respond within two working days. Depending on the incident nature, other CESNET units may be involved, such as the Network Operating Centre (NOC) or the Forensic Laboratory (FLAB). All NOC and FLAB staff are also CESNET employees.

Incidents are prioritized based on their apparent severity.

End users are expected to contact their local network, system or service administrator for assistance. Only limited support can be provided directly to end users.

4.2 Co-operation, Interaction and Disclosure of Information

CESNET-CERTS is a member of the TF-CSIRT community and actively communicates and cooperates with other CERTs/CSIRTs. See: https://csirt.cesnet.cz/en/cooperation.

CESNET-CERTS shares all necessary information with other CSIRTs, as well as with affected network and/or service administrators, in accordance with applicable Czech legislation. It adheres to the Civil Code, the Data Protection, and the Cyber Security Law.

All sensitive data and information (such as personal data, system or service configurations, and vulnerabilities including their locations) are transmitted in encrypted form.

Since 2018, CESNET has implemented an Information Security Management System (ISMS) and has been certified according to ČSN EN ISO/IEC 27001:2023. As part of this certification, rules for information classification and protection are in place. CESNET operates the CESNET-CERTS security team, which includes the FLAB.

4.3 Communication and Authentication

For regular communication that does not contain sensitive information, CESNET-CERTS uses phone or, preferably), unencrypted e-mails with electronic signature. For secure communication, PGP or X.509-based encryption is used.

CESNET-CERTS follows the Traffic Light Protocol (TLP) for classification and distribution of information.

5 Services

CESNET-CERTS provides a range of cybersecurity services in accordance with the CSIRT Services Framework (v2.1) defined by FIRST. The services are organized into the following categories:

5.1 Incident Response

Handling and coordination of cybersecurity incidents within the constituency, including triage, analysis, escalation, and resolution support. CESNET-CERTS addresses both the technical and organizational aspects of incident management.

5.1.1 Incident Triage

- Verifying whether a reported incident is genuine.
- Determining whether the incident is still ongoing or relevant, if possible.
- Assessing the scope and potential impact of the incident.
- Prioritizing incidents according to severity and urgency.

5.1.2 Incident Coordination

- Identifying all organizations involved in the incident.
- Contacting the involved organizations to facilitate investigation and remediation.
- Coordinating with other security teams and relevant stakeholders.
- Facilitating contact with additional parties who can assist in resolving the incident.
- Liaising with appropriate law enforcement authorities, if necessary.

5.1.3 Incident Resolution

- Collecting and preserving evidence related to the incident.
- Providing advice and coordination for containment, eradication, and recovery.
- Maintaining statistics on reported incidents and their resolution.

CESNET-CERTS offers remote guidance and facilitates communication between involved parties but does not provide on-site physical assistance.

5.2 Proactive Activities

Activities aimed at preventing security incidents, improving security posture, and reducing potential impact.

5.2.1 Information Security Event Management

Monitoring and detection of security-relevant events, as well as initial analysis and contextualization using internal and shared systems.

5.2.2 Vulnerability Management

Identification, verification, and analysis of vulnerabilities in systems and networks; includes proactive discovery and coordination of mitigation efforts.

5.2.3 Situational Awareness

Collection and interpretation of data and threat intelligence to improve visibility of risks and trends relevant to the constituency.

5.2.4 Knowledge Transfer

Education and awareness activities focused on strengthening the security posture of the constituency, including training and advisory services.

For more detailed information and a complete overview of CESNET-CERTS services, see: https://csirt.cesnet.cz/en/services.

6 Incident Reporting Forms

No local reporting form is provided. Please follow the general guidelines for submitting an incident report as described on our website:

https://csirt.cesnet.cz/en/incident_report

7 Disclaimers

The security services provided by CESNET are designed to offer significant support in ensuring the cybersecurity of connected organizations. While we strive to deliver high-quality and reliable services, it is not possible to guarantee complete coverage of all security vulnerabilities. Our services should be regarded as a supplement to an organization's own security management, not as a replacement for it. The constituents bear the ultimate responsibility for securing their own environment.