CSIRT description for

CESNET-CERTS

the CESNET, a.l.e. security team

1. Document Information

This document contains a description of CESNET-CERTS team according to RFC 2350. The document provides basic information about the team, the ways it can be contacted, describes its constituency, responsibilities and the offered services.

1.1 Date of Last Update

This is version 1.4, published on March 1, 2018.

1.2 Distribution List for Notifications

There is no distribution list for notifications about changes in this document.

1.3 Locations where this Document May Be Found

The current version of this document can always be found at http://csirt.cesnet.cz.

2 Contact Information

2.1 Name of the Team

CESNET-CERTS

2.2 Address

CESNET, a. l. e.
CESNET-CERTS
Zikova 4
Prague 6
16000
Czech Republic

2.3 Time Zone

Time-zone (relative to GMT): GMT+0100/GMT+0200 (DST).

2.4 Telephone Number

+420 234 680 222

2.5 Facsimile Number

+420 224 320 269

2.6 Other Telecommunication

Twitter: @CESNET_CERTS

2.7 Electronic Mail Address

Please send incident reports to *abuse@cesnet.cz*. To contact the team in other business please use address *certs@cesnet.cz*.

2.8 Public Keys and Encryption Information

The CESNET-CERTS team has a PGP key and each team member uses his/her own PGP key.

CESNET-CERTS team PGP keys:

Master key (used for verification of 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 verification 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

Team representatives PGP keys:

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 keys and their signatures can be found on public keyservers.

2.9 Other Information

General information about CESNET-CERTS can be found at:
http://csirt.cesnet.cz/

CESNET-CERTS posts short messages to the following twitter account:
@CESNET_CERTS

2.10 Points of Customer Contact

The preferred method for contacting CESNET-CERTS team is via e-mail to *abuse@cesnet.cz* (in case of incident reports) or *certs@cesnet.cz* (other business). All e-mails will be handled by the current operator – member of the CESNET-CERTS.

To send us any sensitive information, please use PGP encryption. If e-mail cannot be used or in urgent cases, the phone number given in Paragraph 2.4. can be used on working days between 09:00 and 17:00.

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 as follows:

- To be a Point of Contact for the CESNET network
- To maintain foreign relations with the global community of CERT/CSIRT teams as well as with organizations supporting the community
- To cooperate with various entities across the country – ISPs, content providers, banks, security forces and organizations, institutions in the academic sphere, public authorities and other institutions
- To provide security services such as:
  - Addressing security incidents and coordination thereof
  - Education and tutoring
  - Proactive services in the area of security

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 covers the whole network called CESNET2, i. e., all IP addresses within the AS2852 Autonomous system. The CESNET-CERTS team is fully responsible for handling and responding to security incidents in the domains listed on https://csirt.cesnet.cz/en and in the CESNET2 internal infrastructure marked as INFRA-AW in the RIPE database. CESNET-CERTS can help solve problems in the whole CESNET2 network (AS2852) as well as in the AS48091 Autonomous system.

3.3 Sponsorship and/or Affiliation

The CESNET-CERTS team is established by CESNET, Association of Legal Entities https://www.cesnet.cz. CESNET is an association of Universities and the Academy of Sciences of the Czech Republic. It operates and develops the national e-infrastructure for science, research and education which encompasses a computer network, computational grids, data storage and collaborative environment. It offers a rich set of services to connected organizations.

3.4 Authority

CESNET-CERTS is established by CESNET, Asociation 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 ranges within AS2852 and AS48091.

The level of support given by CESNET-CERTS team depends on the type and severity of the incident, on the type of constituent and the CESNET-CERTS actual resources. In all cases CESNET-CERTS will respond not later than within two working days. Depending on the incident type, some other CESNET unit may be involved, such as NOC (Network Operating Centre) or FLAB (Forensic Laboratory). All members of NOC and FLAB are CESNET emloyees as well.

Basic info about the CESNET Forensic Laboratory: https://flab.cesnet.cz.

Incidents will be prioritized according to their apparent severity.

End users are expected to contact their network/system/service administrator for assistance. Limited support only can be given to the end users.

4.2 Co-operation, Interaction and Disclosure of Information

CESNET-CERTS is a member of the TF-CSIRT community. It communicates and cooperates with other CERTs/CSIRTs.

CESNET-CERTS shares all necessary information with other CSIRTs as well as with affected network and/or service administrators. CESNET-CERTS operates under the restrictions imposed by the Czech law. It follows especially the Civil Code, Data Protection and Cyber Security Law.

All sensitive data and information (personal data, system/service configuration, vulnerabilities with their locations, etc.) are transmitted encrypted.

4.3 Communication and Authentication

For normal communication not containing sensitive information, CESNET-CERTS

uses phone or (preferably) unencrypted e-mails with electronic signature. For secure communication, PGP or X.509 encrypted communication is used.

5 Services

5.1 Incident Response

CESNET-CERTS handles the technical and organizational aspects of incidents. In particular, it provides assistance or advice with respect to the following aspects of incident management:

5.1.1 Incident Triage

- Determining whether an incident is authentic
- Determining whether an incident is still relevant (if possible)
- Assessing and prioritizing the incident.

5.1.2 Incident Coordination

- Determining the involved organizations
- Contacting the involved organizations to investigate the incident and take the appropriate steps
- Facilitating contact to other parties which can help resolve the incident.
- Facilitating contact with other sites which may be involved
- Facilitating contact with appropriate law enforcement officials, if necessary.

5.1.3 Incident Resolution

- Collecting the evidence of the incident.

CESNET-CERTS gives advice, can establish cooperation and communication between involved parties, but cannot provide physical support.

CESNET-CERTS also collects statistics about reported incidents and their solving.

5.2 Proactive Activities

CESNET-CERTS distributes information on misconfigured or otherwise insecure network devices which it gets from its own sources or from third parties. The security information is distributed to appropriate network administrators via the Mentat https://mentat.cesnet.cz and Warden https://warden.cesnet.cz systems.

CESNET-CERTS provides educational services.

6 Incident Reporting Forms

No local form is provided. Please use the basic rules for creating incident report as published on our website:

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

7 Disclaimers

While every precaution has been taken in preparing the information, notifications and alerts, CESNET-CERTS assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.