RFC2350 – description of CSIRT-CEZ

1. Document information

This document contains a description of CSIRT-CEZ according to RFC 2350. It provides basic information about the CSIRT, the ways it can be contacted, describes its responsibilities and the services offered.

1.1 Date of last update

This is the version1 published on 2023/02/07.

1.2 DISTRIBUTION LIST FOR NOTIFICATIONS

There is no distribution list for notifications. Any specific questions or remarks please address to the CSIRT-CEZ mail address.

1.3 LOCATIONS WHERE THIS DOCUMENT MAY BE FOUND

The current version of this CSIRT description document is available from the ČEZ Group website

2. Contact information

2.1 Name of the team

CSIRT-CEZ

2.2 Address

CSIRT-CEZ
Duhová 2/1444
Prague 4, 140 53
Czech Republic

2.3 Time zone

CET, Central European Time (UTC+1, from the last Sunday in October to the last Saturday in March)

CEST, Central European Summer Time (UTC+2, from the last Sunday in March to the last Saturday in October)

2.4 Telephone number

+420 211 042 699 (outside the standard working hours this phone number is redirected to the person on readiness duty)

2.5 FACSIMILE NUMBER

Not available

2.6 Other telecommunication

Not available

2.7 Electronic mail address

For all communication towards CSIRT-CEZ, including incident reports, use the address csirt@cez.cz.

2.8 PUBLIC KEYS AND ENCRYPTION INFORMATION

For the incident related communication, you can use this key:

Type: RSA/3072 Expires: 16.1.2028

Fpr: 12E8 74DE DBF3 4F1F 7EFE 92CB FF1A 27C4 F49B BA2B

UID: CSIRT-CEZ csirt@cez.cz.

2.9 Team members

The team leader of CSIRT-CEZ is Tomáš Grznár. A full list of CSIRT-CEZ members is not publicly available. Team members will identify themselves to the reporting party with their full name in an official communication regarding an incident.

2.10 Other information

The preferred method for contacting CSIRT-CEZ is via e-mail.

If it is not possible (or not advisable for security reasons) to use e-mail, the CSIRT-CEZ can be reached by telephone

The CSIRT-CEZ hours of operation are generally restricted to regular business hours (08:00 - 16:00 Monday to Friday, except holidays). A readiness duty is kept outside the standard working hours.

3. Charter

3.1 Mission statement

Our mission is to contribute to the security of the ICT infrastructure of companies within the ČEZ Group. Our goal is to help them to effectively face security challenges, react on the incidents, coordinate actions to solve them and effectively prevent them.

3.2 Constituency

The constituency of CSIRT-CEZ is composed of all ČEZ Group companies, which access the ČEZ Group´s cyber space and/or use the ICT resources, and which do not have their own capacities and means for handling significant cyber security incidents.

3.3 Sponsorship and/or affiliation

CSIRT-CEZ is a part of the Security department within ČEZ, a. s. (holding company in the ČEZ Group).

3.4 Authority

CSIRT-CEZ has the mandate from the company´s representatives to manage and support the handling of significant groupwide cyber security incidents. CSIRT-CEZ expects to work in close cooperation with the government CERT of the Czech Republic (GovCERT.CZ) and another CERT/CSIRT teams within the ČEZ Group.

4. Policies

4.1 Types of incidents and level of support

CSIRT-CEZ handles the incidents with the origin within the ČEZ Group cyberspace and which have a significant groupwide impact. Groupwide significant incidents are those, which:

- have significant impact on business activities of large number of ČEZ Group companies and/or
- are the result of a long-term coordinated attack targeting the ČEZ Group and/or
- are taking place simultaneously or are the cause of the crisis for which the ČEZ crisis team was activated and/or
- are complex and for mitigation of their impact, it is necessary to take decisions that may have an adverse impact (e.g. limiting connectivity to the Internet, limiting the availability of a large number of key systems) on business activities of a large number of ČEZ Group companies including those companies that were not the direct targets of a cyberattack.

The level of support given by CSIRT-CEZ will vary depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected, and CSIRT-CEZ's resources at the time. Special attention will be given to issues affecting critical information infrastructure.

CSIRT-CEZ will provide mainly the consultancy services and methodological guidance to those companies within the ČEZ Group, which have their own capabilities for cybersecurity incident handling, or which have no access to the ČEZ Group cyberspace.

CSIRT-CEZ is committed to keeping its constituency informed of potential vulnerabilities, and where possible, will inform this community of such vulnerabilities before they are actively exploited.

4.2 CO-OPERATION, INTERACTION AND DISCLOSURE OF INFORMATION

CSIRT-CEZ is ready to cooperate with another trusted security teams (CERT/CSIRT) in the Czech Republic or abroad.

CSIRT-CEZ operates within the bounds of the Czech legislation.

4.3 COMMUNICATION AND AUTHENTICATION

E-mails and telephones are considered sufficiently secure to be used even unencrypted for the transmission of low-sensitivity data. If it is necessary to send highly sensitive data by e-mail, PGP will be used.

If it is necessary to authenticate a person before communicating, this can be done either through existing webs of trust (e.g. TI, FIRST) or by other methods like call-back, mail-back or even face-to-face meeting if necessary.

5. Services

5.1 Incident response

CSIRT-CEZ will assist local administrators in handling the technical and organizational aspects of incidents. In particular, it will provide assistance or advice with respect to the following aspects of incident management:

5.1.1. INCIDENT TRIAGE

- Determining whether an incident is authentic.
- Determining the extent of the incident, and its priority.

5.1.2. INCIDENT COORDINATION

- Contact the involved parties to investigate the incident and take the appropriate steps.
- Facilitate contact to other parties which can help resolve the incident.
- Making reports to other CERT teams or CSIRTs if needed.
- Communicate with stakeholders

5.1.3. INCIDENT RESOLUTION

- Providing advice to another security teams within the ČEZ Group on appropriate actions.
- Follow up on the progress of the concerned security teams within the ČEZ Group.
- Definition of measures/activities to protect another ČEZ Group IT systems and resources from impact of the incident.
- Definition of corrective measures to mitigate the identified vulnerabilities and monitoring the resolution of the corrective measures.

5.2 PROACTIVE ACTIVITIES

CSIRT-CEZ cooperates on several proactive activities to raise security awareness in its constituency.

6. Disclaimer

While every precaution will be taken in the preparation of information, notifications and alerts, CSIRT-CEZ assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.