CSIRT description for

Prazska energetika, a. s. – CSIRT (PRE.CZ-CSIRT)

1. Document Information

This document contains a description of Prazska energetika, a. s. – CSIRT (PRE.CZ-CSIRT) team according to RFC2350. The document provides basic information about the team, the ways it can be contacted, describes its constituance, responsibilities and the offered services.

1.1. Date of Last Update

This is version published on January 5, 2024

1.2. Distribution List for Notification

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 https://csirt.pre.cz

2. Contact Information

2.1. Name of the Team

Official team name: Prazska energetika, a. s. – CSIRT

Nickname: PRE.CZ-CSIRT

2.2. Address

Prazska energetika, a. s. – CSIRT
Na Hroudě 1492/4,
Prague 10, 100 00
Czech Republic

2.3. Time Zone

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

2.4. Telephone Number

+420 721 379 845
+420 267 054 444 (outside working hours)

2.5. Facsimile Number

Not available at this moment.

2.6. Other Telecommunication

Not available at this moment.

2.7. Electronic Mail Address

Please send incident reports to csirt.incident@pre.cz. To contact the team in other business please use address csirt@pre.cz.

2.8. Public Keys and Encryption Information

The PRE.CZ-CSIRT team has a PGP key and each team member uses his/her own PGP key.

PRE.CZ-CSIRT team PGP keys:

Master Key (used for cerifiation of our PGP keys):
User ID: PRE.CZ-CSIRT csirt@pre.cz
Key ID: 0x3629079F

Communication key (used for verification and encryption):
User ID: PRE.CZ-CSIRT csirt.incident@pre.cz
Key ID: 0x38A8F896

Team Representatives PGP keys:

User ID: Jiří Kalousek
Key ID: 0xD62B5B8C
Fingerprint: 5FBD431A71DA2CB4987E8537821BED29D62B5B8C

User ID: Petr Kyndl
Key ID: 0x0BF56CB8
Fingerprint: 0E8DB98393A95F07545BB1DC4073AD0F0BF56CB8

2.9. Other Information

General information about PRE.CZ-CSIRT can be found at: https://csirt.pre.cz

2.10. Points of Customer Contact

The preferd method for contacting PRE.CZ-CSIRT team is via e-mail to csirt.incident@pre.cz (in case of incident reports) or csirt@pre.cz (other business). All e-mail will be handled by the current operator – member of the PRE.CZ-CSIRT. We guarantee a response to an e-mail within 48 hours.

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 9:00-14:00.

3. Charter

3.1. Mission Statement

PRE.CZ-CSIRT is the CSIRT team of PRE group companies.

Main tasks of the team are as follows:

- Triage of security incidents
- To be a point of Contact for PRE group network
- To maintain foreign relations with the global community of CERT/CSIRT and with organizations supporting the community
- To cooperate with other subjects – ISPs, public authorities, content providers, professional groups (CSRES,…)
- Investigating security incidents and their coordination
- Proactive services in the area of security
- Vulnerability scanning services

3.2. Constituency

PRE.CZ-CSIRT is the CSIRT team of PRE group. Its constituency covers the IT part of PRE network. The main mission of PRE.CZ-CSIRT is monitoring and defending external border perimeter of IP addresses within the AS48451 (IPv6: 2a00:f78::/32, IPv4: 94.124.40.0/21). Autonomous system. The PRE.CZ-CSIRT team is fully responsible for handling and responding to security incidents.

3.3. Sponsorship and/or Affiliation

The PRE.CZ-CSIRT team is established by Pražská energetika, a. s.

3.4. Authority

PRE.CZ-CSIRT is established by Pražská energetika, a. s. and is implemented with the aim of ensuring the availability and quality of IT services provided by PRE. Ensures the response to cyber security events and incidents, especially following initiatives from other involved CSIRT teams.

4. Policies

4.1. Type of Incidents and Level of Support

PRE.CZ-CSIRT provides incident handling service for all IP ranges within AS48451 (IPv6: 2a00:f78::/32, IPv4: 94.124.40.0/21).

The level of support given by PRE.CZ-CSIRT team depends on the type and severity of the incidents.

In all cases PRE.CZ-CSIRT will respond within two working days. Depending on the incident type, some other unit may be involved, such as EDR response team or Networking team. All members of EDR and Network teams are consists of employee PRE and his contracted support.

4.2. Co-operation, Interaction and Disclosure of Information

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

PRE.CZ-CSIRT shares all necessary informaiton with other CSIRTs as well as with affected network or service administrators. PRE.CZ-CSIRT operates under the restrictions imposed by the Czech law. It Follows especially the Civil Code, GDPR and Cyber Security Law.

4.3. Communication and Authentication

For normal communication not containing senisitve information, PRE.CZ-CSIRT 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

PRE.CZ-CSIRT handled 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)
- Incident assessment and prioritization

5.1.2. Incident Resolution

- Determining the involved part of administrators/contractors
- Contacting the involved administrators/contractors 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.

PRE.CZ-CSIRT gives advice, can establish cooperation and communication between involved parties, but cannot provide physical support.

PRE.CZ-CSIRT also collects statistics about reported incidents and their solving.

5.2. Proactive Activities

Vulnerability scanning services

6. Incident Reporting Forms

Internal procedure is not public.

Report cyber incident is possible via e-mail adress csirt.incident@pre.cz. It is possible to report cyber incidetn via our webside https://csirt.pre.cz too.

7. Disclaimers

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