CSIRT description for CSIRT.CZ, National CSIRT of The Czech Republic.
==========

1. Document Information

This document contains a description of CSIRT.CZ 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 3.9, published on May 15th 2020.

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 *https://csirt.cz/page/887/contact/*.

2. Contact Information

2.1 Name of the Team

CSIRT.CZ

2.2 Address

CZ.NIC, z. s. p. o. (CSIRT.CZ)
Milešovská 1136/5
Prague 3
130 00
Czech Republic

Contact address:
Hotel Olšanka
Táboritská 23/1000, Prague 3

2.3 Time Zone

Time-zone (relative to GMT): GMT01/GMT02(DST)

2.4 Telephone Number

+420 910 101 010

2.5 Facsimile Number

2.6 Other Telecommunication

None.

2.7 Electronic Mail Address

Please send incident reports to *abuse@csirt.cz*. If you want contact the team with something else than incident report use address *csirt@csirt.cz*.

2.8 Public Keys and Encryption Information

The CSIRT.CZ team has a PGP key and each team member uses its own PGP key. Fingerprints can be found in chapter 2.9.

2.9. Team Members

CSIRT.CZ team has following members - Martin Peterka, Pavel Bašta, Michal Prokop, Edvard Rejthar, Martin Kunc, Petr Špringer, Filip Pokorný, Petra Raszková and Petr Břehovský.

The CSIRT.CZ abuse PGP key:

```
Abuse e-mail address: abuse@csirt.cz
PGP KeyID:  0x6622 A373
Key Fingerprint: 7071 8BB4 0939 AB7D 4E39 4EFD 63A1 D634 6622 A373
```

Team members PGP keys:

```
User ID:     Martin Peterka <martin.peterka@nic.cz>
Key ID:      0xDCEA5E22
Fingerprint: A4BE 75CD B803 E20E 2B75 A7E6 E592 7502 DCEA 5E22

User ID:     Michal Prokop (Csirt CZ) <michal.prokop@csirt.cz>
User ID:     Michal Prokop (Csirt) <michal.prokop@nic.cz>
Key ID:      0xD66EBB7F
Fingerprint: 437D EE6B 90BC FA94 274B C113 4AE0 CC78 D66E BB7F

User ID:     Pavel Basta (Csirt) <pavel.basta@nic.cz>
User ID:     Pavel Basta (Private mail) <pavel@bastovi.com>
User ID:     Pavel Basta (CSIRT.CZ) <pavel.basta@csirt.cz>
Key ID:      0xE0404418
Fingerprint: 433C A7C2 5AB8 0293 3581 7691 A964 C99A E040 4418

User ID:     Edvard Rejthar <edvard.rejthar@csirt.cz>
User ID:     Edvard Rejthar (edvard.cz) <edvard.rejthar@nic.cz>
Key ID:      0xF50BCBD8
Fingerprint: 43B5 C63A E512 2B55 E241  11F6 BA3D 915E F50B CBD8

User ID:     Martin Kunc <martin.kunc@csirt.cz>
Key ID:      0x991CD56E
Fingerprint: 1855 F3B3 6ED7 84A7 DCC1 5556 1EFE 5C6B 991C D56E

User ID:     Petr Springer <petr.springer@csirt.cz>
Key ID:      0xEC0E72D0
Fingerprint: 5AE8 6DCC 2CC3 D1F9 9318 7AF9 9E3C BEB9 EC0E 72D0

User ID:     Filip Pokorny <filip.pokorny@csirt.cz>
Key ID:      0x1371C607
Fingerprint: 3371 5A0E B901 89E5 9241 FA1A 8C16 07AE 1371 C607

User ID:     Petra Raszkova <petra.raszkova@nic.cz>
Key ID:      0xB26D5E0A
Fingerprint: F9F1 8373 E4AD 6517 66DC D009 4317 24DE B26D 5E0A

User ID:     Petr Brehovsky <petr.brehovsky@nic.cz>
Key ID:      0x209ACF7D
Fingerprint: E309 E132 13F3 021D 22F5 5949 DD8D 9FB1 209A CF7D
```

All keys and its signatures can be found at the public keyservers.

2.10 Other Information

General information about CSIRT.CZ can be found at:
https://www.csirt.cz/
https://www.nic.cz/

2.11 Points of Customer Contact

The preferred method for contacting CSIRT.CZ team is via e-mail to *abuse@csirt.cz* (in case of incident reports) or info*@csirt.cz* (other bussiness). All

e-mails will be handled by the responsible human – member of CSIRT.CZ.

If you need to send any sensitive information, use PGP encryption. If it is not possible to use e-mail, or in urgent cases, you can use phone number +420 910 101 010. Days/Hours of Operation: 09:00 to 17:00 Monday to Friday.

Outside the working hours please use emergency nr. +420 222 745 111.

3. Charter

3.1 Mission Statement

CSIRT.CZ is the National CSIRT of the Czech Republic. Main tasks of CSIRT.CZ in the Czech Republic are as follows:

- To be a Point of Contact.
- 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

CSIRT.CZ also handles incidents that originate in networks provided in the Czech Republic and are reported to the team by any person or institutions.

3.2 Constituency

The CSIRT.CZ team constituency is the territory of the Czech Republic, i.e. all users and networks operated in the Czech Republic fall under the responsibility of CSIRT.CZ.

3.3 Sponsorship and/or Affiliation

Team CSIRT.CZ is operated by CZ.NIC, Association of Legal Entities (https://www.nic.cz/). CZ.NIC is the .CZ domain name registry.

3.4 Authority

CSIRT.CZ is provided by CZ.NIC, Association of Legal Entities, and operates with

authority delegated by association and with respect to public agreement, which was concluded between National Security Authority (http://www.nbu.cz/) and CZ.NIC, Association of Legal Entities, on 18 Dec 2015:

All members of CSIRT.CZ are employees of CZ.NIC, Association of Legal Entities.

CSIRT.CZ does its best for cooperation with all large Czech ISP's abuse teams, establish direct contacts and exchange necessary data in order to prevent and recover from security incidents that affect their networks.

4. Policies

4.1 Types of Incidents and Level of Support

CSIRT.CZ provides incident handling service for all IP ranges assigned to the Czech Republic (all network provided in the Czech Republic).

The level of support given by CSIRT.CZ depends on the type and severity of the incident and the type of constituent, and the CSIRT.CZ actual resources. Though in all cases some response will be made within two working days.

Incidents will be prioritized according to their apparent severity.

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

Categories of severity:

a. Low
Typical features:

- difficult verifiable/ identifiable target, requires potential additional investigation of the administrator of service

Impact:

- incidents with a low level of dangerousness
- possibly additionally in such an amount that it does not matter to exact a reaction

Response:

- not necessary, voluntary

Addressees:

- Level 0

Examples:

- random scan port (typing error in the address)
- bulk spam (spam)
- unrequested bounce message
- keylogger (where the service manager must identify the target/aim)
- uncertain hack/ crack /virus /worm

b. Medium

Typical features:
- incidents with a obvious target
- recurrent incidents from the same source or with the same aim

Impact:
- threat for one or several devices

Response:
- may be required (will be clearly asked) within 48 hours

Addressees:
- Level 0, in case of escalation Level 1

Examples:
- apparent port scan, portsweep
- a keylogger where the attacked target is known
- hack/ crack
- deliberately malicious software (malware/ Trojan horse)
- virus / worm
- bulk spam, especially phishing/ pharming mail

c. High

Typical features:
- the suspicious device is obviously a part of the botnet
- distributed or cooperative character
-

Impact:
- mass threat
- damage of a major part (of company)
- violation of the law above the possible minimal treshold of the criminal offense

Reaction:
- within 24 hours

Addressees:
- Level 0 and Level 1 at the same time

Examples:
- DoS/ DDoS

- phishing/ pharming page
- abuse of the copyright
- illegal content in general

d. Critical

Typical features:
- organized crime, international crime
- felony

Impact:
- high social dangerousness
- mass threat in a wide range

Reaction:
- ASAP

Addressees:
- Level 0 and Level 1 at the same time

Examples:
- child abusing materials
- phishing

4.2 Co-operation, Interaction and Disclosure of Information

CSIRT.CZ is a member of TF-CSIRT and FIRST community and communicate and cooperate with other CSIRTs.

CSIRT.CZ exchanges all necessary information with other CSIRTs as well as with affected network/services administrators. CSIRT.CZ operates under the restrictions imposed by Czech law. It involves especially Civil code and Data Protection law.

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

4.3 Communication and Authentication

For normal communication (not containing sensitive information) CSIRT.CZ uses unencrypted e-mails or phone. For secure communication PGP-Encrypted communication is used.

5. Services

5.1 Incident Response

CSIRT.CZ will handle 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 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.

CSIRT.CZ will give advice, can established cooperation and communication between involved parties, but no physical support.

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

5.2 Proactive Activities

CSIRT.CZ provides proactive services in area of warning and alerts.

CSIRT.CZ provides educational services. List of other services provided by CSIRT.CZ is available here.

6. Incident Reporting Forms

The form for reporting the incidents is available here. For more information about

reporting the incident please follow our guidance.

7. Disclaimers

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