

=====

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 1.0, published on 22 Sep 2011.

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://www.csirt.cz/>.

2. Contact Information

2.1 Name of the Team

CSIRT.CZ

2.2 Address

CSIRT.CZ
CZ.NIC, z.s.p.o.
Americka 23
120 00 Prague 2
Czech Republic

2.3 Time Zone

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

2.4 Telephone Number

+420 222 745 111

2.5 Facsimile Number

+420 222 745 112

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 - Andrea Kropacova, Martin Peterka, Pavel Basta, Michal Prokop.

The CSIRT.CZ team PGP key:

Team e-mail address: *csirt@csirt.cz*
PGP KeyID: 46A050CA
Key size: 1024
Key Fingerprint: 22E9 699B 099E 2226 000A 00A5 013F F6B9 46A0 50CA

Team members PGP keys:

User ID: Andrea Kropacova (CSIRT.CZ) <*andrea@csirt.cz*>

Key ID: 0x28C740DA
Fingerprint: 70CB 1439 7087 560F A863 BDF9 B47B E4A6 28C7 40DA

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

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

2.10 Other Information

General information about CSIRT.CZ can be found at:

<http://www.csirt.cz/>

<http://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 *csirt@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 +420 222 745 111. Days/Hours of Operation: 09:00 to 17:00 Monday to Friday.

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 organisations supporting the community.
- To cooperate with various entities across the country – ISPs, content providers, banks, security organs, 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 provided by CZ.NIC, Association of Legal Entities (<http://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 Memorandum in Computer Security Incident Response Team of The Czech Republic, which was concluded between Ministry of Interior of The Czech Republic and CZ.NIC, Association of Legal Entities on 16 December 2010:

http://www.nic.cz/files/nic/doc/Memorandum_CSIRT.CZ-en.pdf

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

CSIRT.CZ does its best for cooperatin 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.

4.2 Co-operation, Interaction and Disclosure of Information

CSIRT.CZ is a member of TF-CSIRT 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 actual (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 no proactive services in area of warning and alerts yet.

CSIRT.CZ provides educational services.

6. Incident Reporting Forms

There is no local form available yet. Please use our basic rules for creating incident report as published on our website:

<https://www.csirt.cz/page/883/hlaseni-incidentu/>

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.