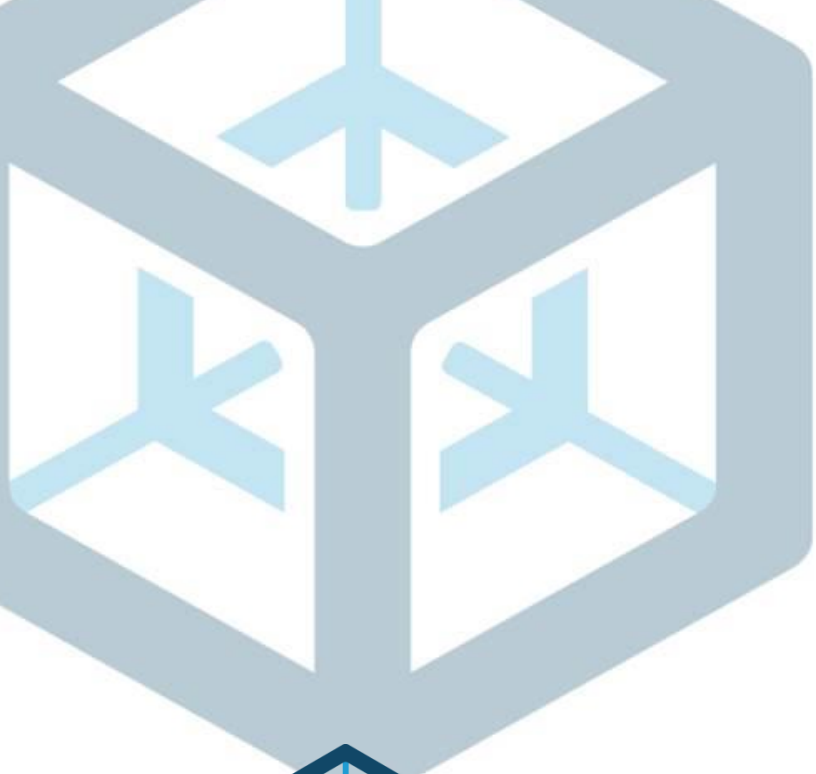

SPCSS

Státní pokladna
Centrum sdílených služeb

CENTRUM
KYBERNETICKÉ BEZPEČNOSTI

RFC 2350

CSIRT-SPCSS

TLP:CLEAR

1. ABOUT THIS DOCUMENT

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

1.1. DATE OF LAST UPDATE

This is version 4 of 12/06/2023

1.2. DISTRIBUTION LIST FOR NOTIFICATIONS

There is no distribution list for notifications. Any specific questions or remarks please address to CSIRT SPCSS s. p. mail address.

1.3 LOCATIONS WHERE THIS DOCUMENT MAY BE FOUND

The current version of this CERT description document is available from the Státní pokladna Centrum sdílených služeb s. p. website.

2. CONTACT INFORMATION

2.1 NAME OF THE TEAM

CSIRT–SPCSS

2.2 ADDRESS

CSIRT–SPCSS

Na Vapence 14

138 00, Praha 3

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

+420 225 515 990

2.5 OTHER TELECOMMUNICATION

Not available

2.6 ELECTRONIC MAIL ADDRESS

For the incident reports, please use the address csirt@spcss.cz

For the non-incident related messages, please use the csirt@spcss.cz

2.7 PUBLIC KEYS AND ENCRYPTION INFORMATION

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

Pub:2048R/3AE09DD9

Fingerprint: 5229 049A 1853 B404 5CDE 1397 D071 F0B7 3AE0 9DD9

2.8 TEAM MEMBERS

The team leader of the CSIRT–SPCSS s. p. is Ondřej Nekovář. A full list of the CSIRT team 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.

2.9 OTHER INFORMATION

General information about the CSIRT-SPCSS can be found at https://www.spcss.cz/csirt/

2.10 POINTS OF CUSTOMER CONTACT

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

Incident reports and related issues should be sent to the address csirt@spcss.cz. This will create a ticket in its tracking system.

For general questions please send an e-mail to csirt@spcss.cz.

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

The CSIRT-SPCSS's hours of operation is provided non-stop, day in and day out.

3. CHARTER

3.1 MISSION STATEMENT

The CSIRT-SPCSS plays a key role in safeguarding the critical information infrastructure of the Státní pokladna Centrum sdílených služeb, s. p. and its customers. Our goal is to help to effectively face security challenges, react on the incidents, coordinate actions to solve them and effectively prevent them.

3.2 CONSTITUENCY

Our constituency is KII SPCSS 01 Bezpecne datove centrum SPCSS (Secure Data Center of SPCSS) a Information systems maintained under ASN AS203165.

3.3 AFFILIATION

CSIRT–SPCSS is part of the state enterprise of Státní pokladna Centrum sdílených služeb s. p., Czech Republic.

3.4 AUTHORITY

The CSIRT-SPCSS operates under the auspices of, and with authority delegated by, Státní pokladna Centrum sdílených služeb s. p. SPCSS s. p. operates within the bounds of the Czech legislation.

The CSIRT-SPCSS expects to work cooperatively with system administrators and users at public sector institutions and at critical information infrastructure, as well as with other entities with a global impact.

4. POLICIES

4.1 TYPES OF INCIDENTS AND LEVEL OF SUPPORT

CSIRT–SPCSS is authorized to address all types of computer security incidents which occur, or threaten to occur, in its constituency.

The level of support given by CSIRT–SPCSS 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–SPCSS's resources at the time, though in all cases some response will be made within one working day. Special attention will be given to issues affecting critical information infrastructure.

Direct support can be given to end users.

CSIRT–SPCSS 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

All incoming information is handled confidentially, regardless of its priority. Information that is evidently very sensitive in nature is only communicated and stored in a secure environment, if necessary using encryption technologies.

CSIRT-SPCSS will use the information you provide to help solve security incidents. Information will only be distributed further to other teams and members on a need-to-know base, and preferably in an anonymized fashion.

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–SPCSS 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 and media

5.1.3. INCIDENT RESOLUTION

- Providing advice to the local security teams on appropriate actions
- Follow up on the progress of the concerned local security teams
- Provide assistance in evidence collection and data interpretation

In addition, CSIRT-SPCSS will collect statistics concerning incidents which occur within or involve its constituency, and will notify the community as necessary to assist it in protecting against known attacks.

5.2 PROACTIVE ACTIVITIES

CSIRT–SPCSS maintains the list of security contacts for every institution in its constituency. Those are available when necessary for solving security incidents or attacks.

CSIRT–SPCSS publishes announcements concerning serious security threats to prevent ICT related incidents or to prepare for such incidents and reduce the impact.

CSIRT–SPCSS is also processing IoCs from available sources and in case of a positive finding ensures propagation of relevant information to the contact responsible for the affected system.

CSIRT–SPCSS also tries to raise security awareness in its constituency.

6. INCIDENT REPORTING FORMS

Incident reporting form is available here:

https://www.spcss.cz/csirt/

An alternative form of reporting (by email to csirt@spcss.cz, by phone at +420 225 515 990), please provide the following information:

- date, time and location of detection
- the name and contact information of the submitter

- the most accurate description of the reported event (how it was detected / recognized, possible causes, existing and estimated impacts / damages)

7. DISCLAIMERS

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