TOTALSERVICE

Description

TOTAL SERVICE CSIRT

(TS CSIRT)

according to RFC 2350 standard

of TOTAL SERVICE a.s.

TOTALSERVICE

Content

Content 2
1. About this document 3
1.1. Date of last update 3
1.2. Notification distribution list 3
1.3. Where this document can be found 3
2. Contact information 3
2.1. Name of the team 3
2.2. Address 3
2.3. Time zone 3
2.4. Telephone number 3
2.5. Fax number 3
2.6. Other communications 4
2.7. E-mail address 4
2.8. Public keys and encryption information 4
2.9. Team members 4
2.10. More information 4
2.11. Contact with the public 4
3. Statutes 5
3.1. Mission 5
3.2. Target group 5
3.3. Classification 5
3.4. Authorization 5
4. Principles 5
4.1. Incident types and level of support 5
4.2. Collaboration, interaction and disclosure 5
4.3. Communication and authentication 6
5. Services 6
5.1. Incidents response 6
5.1.1. Sorting incidents 6
5.1.2. Coordination in incident handling 6
5.1.3. Incident resolution 6
5.2. Proactive attitude 6
6. Incident reporting forms 7
7. Exemption from liability 7

1. About this document

This document contains the description of TOTAL SERVICE CSIRT (TS CSIRT) according to RFC 2350 standard. It provides basic information about TS CSIRT, contact options, responsibilities and services offered.

1.1. Date of last update

This is version number 4 dated 1.6.2021.

1.2. Notification distribution list

There is no notification distribution list. Please send any specific questions or comments to TS CSIRT.

1.3. Where this document can be found

The current version of this TS CSIRT descriptive document is available on the TOTAL SERVICE a.s. (https://www.totalservice.cz), where it can be downloaded.

2. Contact information

2.1. Name of the team

TOTAL SERVICE CSIRT (abbreviated TS CSIRT)

2.2. Address

TOTAL SERVICE a.s. - CSIRT
Metropolitan Building
U Uranie 954/18
170 00 Prague 7
Czech Republic

2.3. Time zone

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

Central European Daylight Time (UTC +2, from last Sunday in March to last Sunday in October)

2.4. Telephone number

+420 270 002 888

2.5. Fax number

Not available

2.6. Other communications

Not available

2.7. E-mail address

To report incidents, please use csirt@totalservice.cz

For other communication please use csirt@totalservice.cz

2.8. Public keys and encryption information

For incident reporting and other communication, please use this key:

User ID: Total Service CSIRT <csirt@totalservice.cz>

PGP KeyID: 0xED27BEEA

Fingerprint: D010 BA0C F8D5 EB99 E83B DA9F 9A33 FCE1 ED27 BEEA

2.9. Team members

TS CSIRT team is headed by Radim Navrátil. The complete list of TS CSIRT team members is not publicly available. Team members identify themselves to the other party with their full name as part of the official incident handling communication.

Management and supervision are provided by the team leader.

2.10. More information

General information about TS CSIRT can be found at www.totalservice.cz

2.11. Contact with the public

The preferred method of contacting TS-CSIRT is via e-mail.

Incident reporting and related issues should be sent to csirt@totalservice.cz. This creates a report in our system.

If it is not possible (or inappropriate for security reasons) to use e-mail, you can contact TS CSIRT by phone.

TS CSIRT working hours are generally limited to normal working hours (8:30-17:00 from Monday to Friday, excluding holidays)

3. Statutes

3.1. Mission

The TS CSIRT team aims to help protect the information infrastructure of its clients and partners. Our goal is to help them effectively address security challenges, respond to incidents, coordinate action for their solution and effectively prevent them.

3.2. Target group

Our target group are mainly clients of TOTAL SERVICE a.s.

We focus on commercial, contributory and non-profit companies and state institutions.

3.3. Classification

TS CSIRT is a part of TOTAL SERVICE a.s., which is its operator.

3.4. Authorization

TS CSIRT works in the private sector within the limits of Czech and European legislation.

TS CSIRT plans to work with system administrators and users within the private and public sector institutions.

4. Principles

4.1. Incident types and level of support

TS CSIRT is authorized to deal with all types of computer security incidents that have arisen or may arise within their jurisdiction.

The level of support provided by TS CSIRT varies depending on the type and severity of the incident or problem, the size of the user community and TS CSIRT resources at the time of the incident, but in any case some type of response will be provided within one business day. Particular attention will be paid to incidents related to critical information infrastructure.

No direct support will be provided to end users. They are expected to work with their system administrator, network administrator or Internet service provider. TS CSIRT will provide them with the necessary support.

TS CSIRT undertakes to inform about potential vulnerabilities and, where possible, to inform the aforementioned target group about such vulnerabilities before they are misused.

4.2. Collaboration, interaction and disclosure

All incoming information is handled safely, regardless of its severity. Visibly highly sensitive information will be processed and stored securely, using encryption technology if necessary.

TS CSIRT will use the information provided to resolve security incidents. Information will be distributed to other teams and members only on a need-to-know basis and, whenever possible, anonymously.

TS CSIRT operates within the limits of Czech legislation.

4.3. Communication and authentication

Unencrypted e-mails and telephones are considered a sufficiently secure way of communicating when transmitting low-sensitive data. If highly sensitive information needs to be sent by e-mail, PGP encryption will be used.

If a person needs to be screened prior to commencing communication, this can be done either through an existing trust network (e.g. TI, FIRST) or by other methods such as callback, e-mail or (if necessary) face-to-face meetings.

5. Services

5.1. Incidents response

TS CSIRT aims to assist local administrators in addressing the technical and organizational aspects of incidents. In particular, it plans to provide assistance or advice on the following aspects of crisis management:

5.1.1. Sorting incidents

- assessing whether the incident is plausible,
- determining the scope of the incident and its priority.

5.1.2. Coordination in incident handling

- Contacting incident stakeholders to investigate the incident and then take appropriate action,
- Facilitate contact with other entities that can help with incident resolution,
- Informing other CERT and CSIRT teams if necessary,
- Communication with stakeholders and the media.

5.1.3. Incident resolution

- Providing advice to local security teams on best practices,
- Tracking the progress of local security teams,
- Providing assistance in gathering evidence and interpreting data.

In addition, TS CSIRT aims to collect statistics on events taking place within its scope, to provide timely information on possible attacks and to help protect against known attacks.

5.2. Proactive attitude

TS CSIRT gathers security contact lists for each institution within its field of competence. These lists are available when needed to deal with security incidents or attacks.

TS CSIRT publishes notifications of serious security threats in order to prevent as far as possible ICT incidents and minimize their impact.

TS CSIRT processes IoC from available sources and, in case of a positive finding, ensures the transmission of relevant information to the contact responsible for the affected system.

TS CSIRT also seeks to raise security awareness within its field of competence.

6. Incident reporting forms

They are not available

7. Exemption from liability

Despite all measures to be taken in the preparation of information, notifications and warnings, TS CSIRT assumes no liability for errors, omissions or damages resulting from the use of the information contained therein.

www.totalservice.cz