1. Document Information
This document provides basic information about the KERNUN CSIRT according to RFC 2350.

1.1 Date of Last Update
This is version 1 of 2017/07/04.

1.2 Distribution List for Notifications
No distribution list for notifications.

1.3 Locations where this Document May Be Found
The current version of this document is available at https://www.kernun.cz/csirt.

2. Contact Information

2.1 Name of the Team
KERNUN CSIRT

2.2 Address
KERNUN CSIRT
Žižkova 600
664 01 Bílovice nad Svitavou
The Czech Republic

2.3 Time Zone
GMT+1 (CET from November to March),
GMT+2 (CEST from April to October)

2.4 Telephone Number
+420 - 545 423 160

2.5 Facsimile Number
Not available

2.6 Other Telecommunication
Skype name: kernun-cz
2.7 Electronic Mail Address
KERNUN CSIRT <csirt@kernun.cz>

2.8 Public Keys and Encryption Information
Each team member uses their PGP key. Information about the personal keys are available in the chapter 2.9. The team PGP key and its fingerprint are:

   Email address: KERNUN CSIRT <csirt@kernun.cz>
   PGP KeyID: 0xD81B6154
   Key Fingerprint: 0679 B642 13D7 7E5B 142C 24F6 13B6 47BD D81B 6154

2.9 Team Members
Josef Vávra
   Email address: Josef Vávra <josef.vavra@kernun.cz>
   PGP KeyID: 0x2DAA2CC0
   Key Fingerprint: 5DB8 943C 57DE D037 3F0C 40C8 2943 AD0C 2DAA 2CC0

Petr Svoboda
   Email address: Petr Svoboda <petr.svoboda@kernun.cz>
   PGP KeyID: 0xE79C9410
   Key Fingerprint: F291 8A69 9567 C3A7 7DF7 52D7 8DEC 0B7C E79C 9410

Jan Pawlik
   Email address: Jan Pawlik <jan.pawlik@tns.cz>
   PGP KeyID: 0x9B1C8096
   Key Fingerprint: 143E A94D 00EB 3D07 1B85 6EFE 7F3E 5B28 9B1C 8096

2.10 Other Information
For other information please see https://www.kernun.cz/csirt.

2.11 Points of Customer Contact
The preferred way to contact KERNUN CSIRT is via e-mail.

If for any reason it is not possible or advisable to use the e-mail, KERNUN CSIRT can be reached at the telephone number stated in the chapter 2.4. The working hours are Monday to Friday 08:00-17:00 (except holidays).
3. Charter

3.1 Mission Statement

KERNUN CSIRT's goals are

- to help customers to face and in-time respond actual threats and attacks concerning mainly the Czech republic,
- to handle incidens that concern customers’ networks,
- to be the point of contact for the customers,
- to keep in touch with other CSIRTs.

3.2 Constituency

Our constituency are the networks of the clients of TNS, a.s. that are under managed services contract, and the TNS networks.

3.3 Sponsorship and/or Affiliation

KERNUN CSIRT is operated by TNS, a.s.

3.4 Authority

KERNUN CSIRT was found by TNS, a.s. and all the members of KERNUN CSIRT are employees of TNS, a.s. KERNUN CSIRT cooperates with the customers on the basis of business contracts.

4. Policies

4.1 Types of Incidents and Level of Support

KERNUN CSIRT provides incident handling concerning Kernun products, IP ranges assigned to the customers of TNS or customers using Kernun products, or to the IP ranges assigned to TNS.

The level of support given by KERNUN CSIRT will vary depending on the type and severity of the incident or issue, the type of the constituent, the type service level of a particular customer, and KERNUN CSIRTs resources at the time, though in all cases some response will be made within one working day.

Incidents will be prioritized according to their severity. Special attention will be given to the issues affecting critical information infrastructure.

Only limited support will be given to end users; they are expected to contact their system administrator, network administrator or their ISP for assistance.
4.2 Co-operation, Interaction and Disclosure of Information
KERNUN CSIRT cooperates and exchanges information with other CSIRTs. Information that is evidently very sensitive in nature is only communicated and stored in a secure environment using encryption technologies.

KERNUN CSIRT operates within the bounds of the Czech laws.

4.3 Communication and Authentication
For normal communication not containing sensitive information an unencrypted email can be used. For secure communication an email encrypted by PGP will be used.

5. Services

5.1 Incident Response
KERNUN CSIRT will handle the technical and organizational aspects of incidents. In particular, it will provide assistance or advice or implement a security measure if possible with respect to the following aspects of incident management:

5.1.1. Incident Triage
  • Determining whether an incident is authentic.
  • Determining whether the incident is still relevant.
  • Determining the extent of the incident and its priority.

5.1.2. Incident Coordination
  • Determining involved organizations.
  • Contacting the organizations to investigate the incident and take the appropriate steps.
  • Facilitate contact to other parties which can help resolve the incident.

5.1.3. Incident Resolution
  • Providing advice to the local security teams on appropriate actions.
  • Securing the infrastructure from the effects of the incident, if possible.
  • Providing assistance in evidence collection and data interpretation.

5.2 Proactive Activities
KERNUN CSIRT will provide warnings and alerts to the customers.

6. Incident Reporting Forms
There is no required format of forms for reporting the incidents, however a report should contain such information:

• Contact and organizational information
• Date and time when the incident was observed.
• Description of the incident containing all relevant data that are at hand.

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