RFC2350

1. Document information

This document contains a description of CS-CIRT team according to RFC 2350. It provides basic information about the team, communication contacts describe its responsibilities and the services offered.

1.1 Date of last update

Document version: 1.3
Last update: 19th of October 2021

1.2 Distribution list for notifications

There is no distribution list for notifications as of 2021/09.

1.3 Locations where this document may be found

The current version of this document is located at www.comsource.cz/csirt

2. Contact information

2.1 Name of the team

CS-CSIRT

2.2 Address

ComSource s.r.o.
Nad Vrsovskou horou 1423/10
101 00 Praha 10

2.3 Time zone

Central European time zone (CET) which is GMT+0100 (+0200 during day-light saving time).

2.4 Telephone number

+420 226 801 755

2.5 Facsimile number

None

2.6 Other telecommunication

None.

2.7 Electronic mail address

Please send incident reports to soc@comsource.cz

2.8 Public keys and encryption information

Every team member use his own PGP key. See list of relevant PGP keys in following chapter 2.9

2.9 Team members

The CS-CIRT team members are Antonin Kovar , Martin Dvorak, Jakub Alimov, Jaroslav Barton , Lukas Harkabus, Lukas Mezera, Lukas Zavadil, Michal Stusak, Otto Krejci, Robert Hroncek, Stefania Sobotova

Team members information:

Antonin Kovar
email: antonin.kovar@comsource.cz
PGP key: 088B 9B37 4ADC 1545 B93C 752B 7F3F 762D 5237 D74D

Martin Dvorak
email: martin.dvorak@comsource.cz
PGP key: 6FB5 B7B1 EDC1 2029 7CB2 A497 BB75 E1EE EE6A 443B

Jakub Alimov
email: jakub.alimov@comsource.cz
PGP key: EBF9 2802 15D9 F206 8295 E691 9A08 C934 7D79 C3B8

Jaroslav Barton
email: jaroslav.barton@comsource.cz
PGP key: B19B D8A1 AA3E 111C D41A FAC4 4C54 873B 2E66 7D2E

Lukas Harkabus
email: lukas.harkabus@comsource.cz
PGP key: 7715 36AB 8269 0B04 171F 0A86 2942 8597 4418 C5D5

Lukas Mezera
email: lukas.mezera@comsource.cz
PGP key: C2B5 4B8F A0B3 4B67 CBC5 DE35 F6C7 BD37 D385 29FC

Lukas Zavadil
email: lukas.zavadil@comsource.cz
PGP key: D001 FEFE 9330 3874 F5D2 A57C DAF6 B3D5 8DF4 127A

Michal Stusak
email : michal.stusak@comsource.cz
PGP key: 434B 2800 7D52 57B4 911C A4EE 14EC 8C6E 1B09 A6FA

Otto Krejci
email : otto.krejci@comsource.cz
PGP key: 0393 6A59 5176 D758 1CB6 7FA9 2D8B FFE3 5EA4 C9B1

Robert Hroncek
email : robert.hroncek@comsource.cz
PGP key: 9504 5611 DE5A 7806 8BAA 7BCE F699 395E 1AF3 E34E

Stefania Sobotova
email: stefania.sobotova@comsource.cz
PGP key: 7E16 7471 7390 EC11 7AD9 722B 5BF8 0DCD 9DDF 60BA

2.10 Other information
None

2.11 Points of customer contact
The preferred method to contact CS-CIRT teams is to send an email to email address soc@comsource.cz This will create a ticket in our tracking system and alert the human on duty. In urgent cases you can contact us by calling +420226801755.
Hours of operation: Monday-Friday, 8 a.m. - 5 p.m

3. Charter

3.1 Mission statement
The purpose of CS-CIRT team is to solve security incidents response for IT-security problems within autonomous system AS199803

3.2 Constituency
CS-CIRT team constituency covers the AS199803 autonomous system and solves security incidents in following domains:
comsource.cz
flowguard.io

3.3 Sponsorship and/or Affiliation
CS-CIRT team is department of Comsource s.r.o.

3.4 Authority
CS-CIRT is department of Comsource s.r.o. and operates with authority delegated by the company. As described in chapter 3.1, team is responsible for solving incidents within autonomous system AS199803.

4.Policies

4.1 Types of Incidents and Level of Support

CS-CSIRT is authorized to address all types of security incidents which occur, or threaten to occur, in our constituency (see 3.2) and require cross-organizational coordination. The level of support given by CS-CSIRT 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 our resources at the time. Special attention will be given to issues related to DDoS incidents.

4.2 Co-operation, Interaction and Disclosure of Information

CS-CSIRT is ready to cooperate with other organizations and teams.
We operate under the restrictions imposed by Czech law. It involves especially Civil code and Data Protection law.

4.3 Communication and Authentication

For normal communication not containing sensitive information we use unencrypted e-mail. For secure communication PGP-Encrypted e-mail will be used.

5. Services

5.1 Incident response

CS-CSIRT will assist IT-security teams in handling the technical and organizational aspects of incidents and 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
- assessing and prioritizing the incident

5.1.2. Incident coordination

- determine the involved organizations
- contact the involved organizations to investigate the incident and take the
- appropriate steps
- facilitate contact to other parties which can help resolve the incident
- share incident information with other CSIRT teams

5.1.3. Incident resolution

- provide resolution or reported security incident or issue
- follow up on the progress of the concerned local security teams
- secure the system from the effect of reported incident
- collect information

5.2 Proactive activities

CS-CSIRT do not pursue proactive activities.

6. Incident reporting forms

There are no local forms available.
Incident's information, details are tracked and reported in incident management System.

7. Disclaimers

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