Description for the

ELAT CSIRT

Table of contents

2 ABOUT THIS DOCUMENT

This document contains a description for the ELAT CSIRT sccording to RFC 2350. It provides basic information about the CSIRT team, the ways it can be contacted, describes its responsibilities and the services offered.

1.1 DATE LAST UPDATED

This is version number 1 of 2018/03/15.

1.2 DISTRIBUTION LIST FOR NOTIFICATION

There is no distribution list for notifications. Any specific questions or remarks please address to the ELAT CSIRT TEAM.

1.3 LOCATIONS WHERE THIS DOCUMENT MAY BE FOUND

The current version of the descriptive document is available on the website https://www.elat.cz/csirt

3 CONTACT INFORMATION

2.1 NAME OF THE TEAM

ELAT CSIRT

2.2 ADDRESS

ELAT s.r.o. - CSIRT
Československého exilu 1888/4
14300, Praha 12 - Modřany
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 541225561
+420 725858296

2.5 FASCIMILE NUMBER

Not available

2.6 OTHER TELECOMMUNICATION

Not available

2.7 ELECTRONIC MAIL ADDRESS

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

2.8 PUBLIC KEYS AND ENCRYPTION INFORMATION

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

Team key ID: E5245F9C

<csirt@elat.cz>

Key fingerprint = 11EC 5F6E 9AC3 E2E0 1185 BC41 44AE 2800 E524 5F9C

2.9 TEAM MEMBERS

Lukáš Vondráček – team leader
lukas.vondracek@elat.cz
PGP key ID:0xAC6D3E23

Jiří Richter – deputy team leader
jiri.richter@elat.cz
PGP key ID:0x5DB192F4

A full list of 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.

Management, liaison and supervision are provided by team leader.

2.10 OTHER INFORMATION

General information about the ELAT CSIRT can be found at
https://www.elat.cz/csirt .

2.11 Points of Customer Contact

The preferred method for contacting ELAT CSIRT is via e-mail.
Incident reports and related issues should be sent to the address
csirt@elat.cz . This will create a ticket in our tracking system.

If it is not possible to use e-mail, the ELAT CSIRT can be reached by phone.

The ELAT CSIRT hours of operation are generally restricted to regular business hours (09:00-17:00 Monday to Friday, except of holidays).

4 CHARTER

3.1 MISSION STATEMENT

ELAT CSIRT team aims to help protect the information infrastructure of their clients and partners. Our goal is to help them effectively address security challenges, respond to incidents, coordinate steps to address them, and effectively prevent them.

3.2 CONSTITUENCY

Our target group is primarily our clients. We focus on commercial, contributory and state-established entities, including the public sector institutions in the Czech Republic.

3.3 SPONSORSHIP AND/OR AFFILIATION

ELAT CSIRT is part of the ELAT s.r.o.

3.4 AUTHORITY

ELAT CSIRT team works in the private sector within the limits of Czech and EU legislation.

ELAT CSIRT team plans to work with system administrators and users within private and public sector institutions.

5 POLICIES

4.1 TYPES OF INCIDENTS AND LEVEL OF SUPPORT

The ELAT CSIRT team is authorized to address all types of computer security incidents which occur, or threaten to occur, in our constituency.

The level of support given by ELAT CSIRT team 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 ELAT CSIRT team 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.

Note that no direct support will be given to end users; they are expected to contact their system administrator, network administrator or their ISP for assistance. The ELAT CSIRT team will support the latter people.

The ELAT CSIRT team 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 by ELAT CSIRT team, 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.

The ELAT CSIRT team 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. The ELAT CSIRT team operates within the bounds of the Czech and EU legislation.

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.

6 SERVICES

5.1 INCIDENT RESPONSE

ELAT CSIRT team 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, the ELAT CSIRT 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

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

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

ELAT CSIRT is also processing IoCs1 from available sources and in case of a positive finding ensures propagation of relevant information to the contact responsible for the affected system.

ELAT CSIRT also tries to raise security awareness in its constituency.

7 THE FORM FOR REPORTING INCIDENTS

Not available

8 DISCLAIMERS

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