DESCRIPTION OF THE GOVERNMENT CERT OF THE CZECH REPUBLIC

1. ABOUT THIS DOCUMENT

This document contains a description of the Government CERT of the Czech Republic according to RFC 2350. It provides basic information about the CERT, the ways it can be contacted, describes its responsibilities and the services offered.

1.1 DATE OF LAST UPDATE

This is version 12 from 2020/08/17.

1.2 DISTRIBUTION LIST FOR NOTIFICATIONS

There is no distribution list for notifications. Any specific questions or remarks please address to the GovCERT.CZ mail address.

1.3 LOCATIONS WHERE THIS DOCUMENT MAY BE FOUND

The current version of this CERT description document is available from the NUKIB website – download here

2. CONTACT INFORMATION

2.1 NAME OF THE TEAM

GovCERT.CZ: Government CERT of the Czech Republic

2.2 ADDRESS

National Cyber Security Centre (Government CERT)
Mucednicka 1125/31
616 00, Brno
Czech Republic

2.3 TIME ZONE

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

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

2.4 TELEPHONE NUMBER

+420 541 110 777

+420 725 502 878 (outside of working hours)

2.5 FACSIMILE NUMBER

+420 257 283 580

2.6 OTHER TELECOMMUNICATION

None available

2.7 ELECTRONIC ADDRESS

For incident reports, please use the address cert.incident@nukib.cz.

For non-incident related messages, please use cert@nukib.cz.

2.8 PUBLIC KEYS AND ENCRYPTION INFORMATION

For incident related communication, you can use this key:

```
pub  4096R/D2A1C881 2019-08-01
uid Government CERT Incident CZE (Reporting channel for NCSC CZE)
<cert.incident@nukib.cz>
Key fingerprint = 3F29 12FE 999B 93D9 AB58 DC5C 43A1 3897 D2A1 C881
```

For non-incident related communication, you can use this key:

```
pub  4096R/A57337A6 2019-08-01
uid Government CERT CZE (Communication channel with NCSC CZE)
<cert@nukib.cz>
Key fingerprint = F60C 0622 EE75 52C9 7EE5 E9F8 4405 4AC1 A573 37A6
```

2.9 TEAM MEMBERS

The team leader and the Director of the GovCERT.CZ Department is Jakub Vesely. A full list of GovCERT.CZ 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 Lukas Kintr, the Deputy Director of National Cyber Security Centre Division, National Cyber and Information Security Agency.

2.10 OTHER INFORMATION

General information about the GovCERT.CZ can be found at www.nukib.cz/en/.

2.11 POINTS OF CUSTOMER CONTACT

The preferred method for contacting GovCERT.CZ is via e-mail.

Incident reports and related issues should be sent to the address cert.incident@nukib.cz. This will create a ticket in our tracking system. In case of reporting incident outside of working hours also contact the person on duty at +420 725 502 878.

For general questions please send an e-mail to cert@nukib.cz.

In case it is not possible (or not advisable for security reasons) to use e-mail, the GovCERT.CZ can be reached by telephone.

The GovCERT.CZ's hours of operation are generally restricted to regular business hours (07:45-16:30 Monday to Friday except holidays).

3. CHARTER

3.1 MISSION STATEMENT

The Government CERT plays a key role in safeguarding the critical information infrastructure and the state bodies. Our goal is to help them to effectively face security challenges, react to incidents, coordinate actions to solve them and effectively prevent them.

3.2 CONSTITUENCY

Our constituency are public sector institutions and critical information infrastructure of the Czech Republic.

3.3 SPONSORSHIP AND/OR AFFILIATION

GovCERT.CZ is part of the National Cyber Security Centre, National Cyber and Information Security Agency, Czech Republic.

3.4 AUTHORITY

The Government CERT operates under the auspices of, and with authority delegated by, the National Cyber Security Centre. The National Cyber Security Centre operates within the bounds of the Czech legislation.

The GovCERT.CZ expects to work cooperatively with system administrators and users in public sector institutions and in critical information infrastructure.

4. POLICIES

4.1 TYPES OF INCIDENTS AND LEVEL OF SUPPORT

The GovCERT.CZ 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 GovCERT.CZ 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 GovCERT.CZ'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.

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. GovCERT.CZ will support the latter people.

GovCERT.CZ 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 GovCERT.CZ, regardless of its priority. Information that is evidently very sensitive in nature is only communicated and stored in secure environment, if necessary using encryption technologies.

GovCERT.CZ 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 basis, and preferably in an anonymized fashion. The GovCERT.CZ operates within the bounds of the Czech 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.

5. SERVICES

5.1 INCIDENT RESPONSE

GovCERT.CZ will assist local administrators in handling the technical 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, GovCERT.CZ will collect statistics concerning incidents which occur within or involve its constituency, and it will notify the community as necessary to assist it in protecting against known attacks.

5.2 PROACTIVE ACTIVITIES

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

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

GovCERT.CZ is also processing IoC[1] from available sources and in case of a positive finding ensures propagation of relevant information to the contact responsible for the affected system.

GovCERT.CZ also tries to raise security awareness in its constituency.

6. INCIDENT REPORTING FORMS

The form is available here

XML schema is available here (only in Czech)

7. DISCLAIMERS

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

[1] Indicator of Compromise