RFC 2350 STANDARD

DESCRIPTION OF CSIRT team DCeGOV.

1. ABOUT THIS DOCUMENT

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

1.1 DATE OF LAST UPDATE

This is version 2 of 28/11/2024.

1.2 DISTRIBUTION LIST FOR NOTIFICATIONS

There is no distribution list for notifications. Any specific questions or remarks please address to the CSIRT DCeGOV team mail address.

1.3 LOCATIONS WHERE THIS DOCUMENT MAY BE FOUND

The current version of this document is available from this location: www.nakit.cz/csirt.

2. CONTACT INFORMATION

2.1 NAME OF THE TEAM

CSIRT DCeGOV

2.2 ADDRESS

CSIRT DCeGOV

Národní agentura pro komunikační a informační technologie, s. p.

Kodaňská 1441/46

101 00 Praha 10 – Vršovice

Czechia

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

+420.974.801.250 (please mention CSIRT team)

2.5 FACSIMILE NUMBER

Not available.

2.6 OTHER TELECOMMUNICATION

Not available.

2.7 ELECTRONIC MAIL ADDRESS

For both incident reports and for non-incident related messages, please use the address csirt-dcegov@nakit.cz.

2.8 PUBLIC KEYS AND ENCRYPTION INFORMATION

For incident and non-incident related communication, you can use this public key of CSIRT DCeGOV team:

```
Key ID: D142 2982 7DBB B50C
```

```
Fingerprint: AF91 5EA6 45F4 3836 FC2D 0C02 D142 2982 7DBB B50C
```

2.9 TEAM MEMBERS

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 and supervision of CSIRT DCeGOV is provided by NAKIT (Národní agentura pro komunikační a informační technologie).

2.10 OTHER INFORMATION

General information about CSIRT DCeGOV can be found at www.nakit.cz.

2.11 POINTS OF CUSTOMER CONTACT

The preferred method for contacting CSIRT DCeGOV is via e-mail.

Incident reports as well as general inquiries should be sent to the address csirt-dcegov@nakit.cz. In case of urgent incident reporting both inside and outside of working hours please call +420 974 801 250 and mention CSIRT to the person on duty. Hours of operation are 7am to 7pm Central European Time (GMT+1), Monday to Sunday, including public holidays of Czech Republic.

3. CHARTER

3.1 MISSION STATEMENT

CSIRT DCeGOV team helps protecting critical infrastructure of systems owned and managed by the Ministry of the Interior and other Czech government entities. List of these systems is not publicly available.

CSIRT DCeGOV team handles the most critical cybersecurity incidents (most often incidents of category II. and III. according to ISMS MV ČR methodology).

3.2 CONSTITUENCY

Our constituency is Ministry of the Interior of the Czech Republic (MV ČR) as well as other customers of DCeGOV.

3.3 SPONSORSHIP AND/OR AFFILIATION

CSIRT DCeGOV is sponsored by Ministry of the Interior of the Czech Republic (MV ČR).

3.4 AUTHORITY

CSIRT DCeGOV operates under the auspices of Ministry of the Interior of the Czech Republic (MV ČR).

4. POLICIES

4.1 TYPES OF INCIDENTS AND LEVEL OF SUPPORT

CSIRT DCeGOV 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 CSIRT DCeGOV 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 CSIRT DCeGOV 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 in most cases, no direct support will be given to end users; they are expected to contact their system administrator, network administrator or their ISP for assistance.

CSIRT DCeGOV 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 CSIRT DCeGOV, 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.

CSIRT DCeGOV 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. CSIRT DCeGOV 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.

5. SERVICES

5.1 INCIDENT RESPONSE

CSIRT DCeGOV will assist local administrators in handling the technical and organizational aspects of incidents. 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.
- Communicate with stakeholders.

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, CSIRT DCeGOV 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

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

CSIRT DCeGOV is also processing indicators of compromise (IoCs) from available sources and in case of a positive finding ensures propagation of relevant information to the contact responsible for the affected system.

6. INCIDENT REPORTING FORMS

When reporting incident, please ensure to include the following information:

- Person reporting given incident: name, email address, phone number, affiliation.
- Name of affected system and its owner.
- Description of the problem: what the expected behavior is vs. what the observed (problematic) behavior is.
- Beginning and end of observed behavior of affected system.
- Any additional context as appropriate.

7. DISCLAIMERS

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