RFC 2350 Document for TMCZ CSIRT

1. Document Information
1.1 Date of Last Update
This is version 3.00, published 2025/01/14

1.2 Distribution List for Notifications
csirt@t-mobile.cz

1.3 Locations where this Document May Be Found
The current version of this CSIRT description document is available on TMCZ CSIRT website, at: http://cert.t-mobile.cz/rfc2350
Please make sure you are using the latest version

2. Contact Information
2.1 Name of the Team
TMCZ CSIRT

2.2 Address
TMCZ CSIRT / Martin Štalmach
T-Mobile Czech Republic a.s.
Tomíčkova 2144/1
148 00 Praha 4

2.3 Time Zone
GMT +0100 - Central European Time (CET)
GMT +0200 - Daylight Saving Time (from last Sunday in March to last Sunday in October)

2.4 Telephone Number
+420 603 603 655 (24x7 CSIRT hotline)

2.5 Facsimile Number
None available

2.6 Other Telecommunication
None available

2.7 Electronic Mail Address
csirt@t-mobile.cz

2.8 Public Keys and Encryption Information
TMCZ CSIRT uses PGP key, which is publicly available at
http://cert.t-mobile.cz/teamCSIRT/CSIRT_PGP_public_key.zip
Key fingerprint: 2A0C BAF9 0B9C 25D9 500F 5E9B E681 FBF5 9FC9 F165

2.9 Team Members
The team leader of TMCZ CSIRT is Martin Štalmach. A full list of the 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.

2.10 Other Information
General information about TMCZ CSIRT team can be found at TMCZ CSIRT website at: http://cert.t-mobile.cz/teamCSIRT

2.11 Points of Customer Contact
The preferred method for contacting the TMCZ CSIRT is by e-mail csirt@t-mobile.cz. An e-mail sent to this address will be handled by a responsible person from CSIRT team.
If it is not possible to use e-mail, TMCZ CSIRT can be reached by 24x7 SOC hotline +420 603 603 655.
TMCZ CSIRT’s hours of operation are generally restricted to regular business hours (09:00-17:00 Monday to Friday except holidays).

3. Charter
3.1 Mission Statement
The purpose of the TMCZ CSIRT is to assist users of T-Mobile Czech Republic network in implementing proactive measures to reduce the risks of computer security incidents, and to assist users of T-Mobile Czech Republic network in responding to such incidents when they occur.

3.2 Constituency

TMCZ CSIRT constituency is all users and organizations of T-Mobile Czech Republic (contains all systems connected to T-Mobile Czech Republic network: AS5588, AS12767, AS13036)
Note however, that due to nature of provided services to users of T-Mobile Czech Republic network, different Level of Support is given to different types of constituents (please, check Section 4.1 and Section 5.1 for more details)
TMCZ CSIRT divides constituents into 3 types:
- backbone network infrastructure of T-Mobile Czech Republic, it's employees and associates; also referred as „internal T-Mobile infrastructure" in further part of Document
-companies, for which T-Mobile Czech Republic provides services in B2B model; also referred as „B2B customer" in further part of Document
- individual customers, to which T-Mobile Czech Republic provides services; also referred as "individual customers" in further part of Document

3.3 Sponsorship and/or Affiliation
TMCZ CSIRT is fully sponsored by T-Mobile Czech Republic.

3.4 Authority
The TMCZ CSIRT operates under the auspices of, and with authority delegated by, the management of T-Mobile Czech Republic.

4. Policies
4.1 Types of Incidents and Level of Support
Level of support given by TMCZ CSIRT will vary depending on type of the constituent, the type and severity of the issue, the size of the user community affected and TMCZ CSIRT resources at the time.
TMCZ CSIRT will generally accept any incident report that involves an incident with one of the constituents either as a victim or as a suspect. However, only in cases when report concerns internal T-Mobile Czech Republic infrastructure, TMCZ CSIRT is able to handle the incidents. For individual and B2B customers, incident response is limited to critical situation.
Resources will be assigned according to the following priorities, listed in decreasing order:
- root or system-level attacks on any Management Information System, or any part of T-Mobile Czech Republic backbone network infrastructure or attacks on any large public service machine;
- compromise of restricted confidential service accounts or software installations, compromise of confidential data or integrity, also used for system administration;
- denial of services attacks or any other attempts of limiting availability of service or information (especially massive distributed attacks) on any of the above 3 items;
- any of the above malicious actions at other sites, originating from backbone network infrastructure;
- large-scale attacks of any kind, e.g. "social engineering" attacks, password cracking attacks;
- other security-related issues, e.g. malware occurrence, e-mail spam etc.
All incident reports are verified manually by a TMCZ CSIRT team member and response to the reporter is made within next business day.

4.2 Co-operation, Interaction and Disclosure of Information
TMCZ CSIRT respects TLP as well as T-Mobile Czech Republic Privacy Policy, and treats all information accordingly to its sensitivity status.
TMCZ CSIRT may share information submitted on a need-to-know basis with trusted parties (other CERT teams, other ISPs) for the sole purpose of incident handling.
TMCZ CSIRT declares full support for the Information Sharing Traffic Light Protocol (https://www.trusted-introducer.org/ISTLPv11.pdf). Information sent in and labelled according to ISTLP will be handled appropriately.

4.3 Communication and Authentication
TMCZ CSIRT uses PGP encryption for communication to ensure integrity and confidentiality.
Main communication channel is e-mail, and messages sent by TMCZ CSIRT staff would be signed with main PGP key (see Section 2.1). Should message contain any sensitive information, it would be additionally encrypted.

5. Services

5.1 Incident Response
TMCZ CSIRT will assist system 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
The main goals of incident triage are:
- investigating whether indeed a security incident occurred,
- determining the extent and severity of the incident (including a potential impact on the constituency), etc.
This service is served to every type of constituent.

5.1.2 Incident Coordination
The goal follow is to provide a complex coordination incidents with particular emphasis on exchanging information between various involved parties. These include but are not limited to:
- determining the initial cause of the incident (exploited vulnerability),
- facilitating contact with other sites which may be involved,
- facilitating contact with appropriate security teams and/or law enforcement officials if necessary,
- making reports to other CSIRTs, if applicable
- composing announcements to users (members of the constituency), if applicable.
Due to limited resources, this service is primarily served for internal TMobile infrastructure and B2B customers.
In very rare critical situations, incident coordination is provided to individual customers.

5.1.3. Incident Resolution
The incident resolution only is performed in limited range for internal TMobile infrastructure only.

5.2 Proactive Activities
TMCZ CSIRT coordinates and maintains the following services to the extent possible depending on its resources:
- Information services Repository of security tools and documentation for use by employees of T-Mobile Czech Republic.
- Training services TMCZ CSIRT will give periodic seminars on computer security related topics; these seminars are available to employees and B2B customers of T-Mobile Czech Republic.

6. Incident Reporting Forms
There are no local forms developed for reporting incidents to TMCZ CSIRT.

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