RFC 2350 CIRT.ME

1. Document information

This document contains information and describe responsibilities, services, and other information about CIRT.ME. The document complies with the reuirements of RFC 2350 (https://www.ietf.org/rfc/rfc2350.txt)

1.1.Date of last update:

This is version 2.00, published in December 2021.

1.2.Distribution list for notifications

There is currently no distribution list for notifications about the document change.

1.3.Locations where this document may be found

The current version is available on CIRT.ME website on the following link.

1.4.Authenticating

- Title: "RFC2350 CIRT.ME"
- Version: 2.00
- Document date: December 2021
- Expiration: This document is valid until further notice

2. Contact Information

2.1.Name of the team

Full name: CIRT.ME - Computer Incident Response Team of the Montenegro

2.2.Team HQ address:

CIRT.ME
Cetinjska 11, The Capital Plaza, The Business Tower
81000 Podgorica
Montenegro

2.3.Team time zone:

CET Central European Time (UTC+01:00)

2.4.Team contact telephone number:

+382 20 247 863

2.5.Team facsimile number:

There's none available.

2.6.Other telecommunication:

There's none available.

2.7.Electronic mail address

kontakt@cirt.me - for incident reporting
info@cirt.me - for other communication

2.8.Public keys and other encryption information:

For encrypted communication CIRT.ME uses PGP key.
Information about the key:
Key fingerprint = 6A931425BCD543B5E06ECE1774545C86B7209F7D

2.9.Team members

Full list of CIRT members is not publicly available.

2.10. Other information:

General information about the CIRT.ME, as well as links to various recommended security resources can be found at: www.gov.me/cirt
Facebook: (https://www.facebook.com/cirt.me)
Instagram: (https://www.instagram.com/cirt.me)
Twitter: (https://twitter.com/CIRT_ME)
Youtube: (https://www.youtube.com/@CIRTME)

2.11. Point of contact:

Primary communication method for is via e-mail kontakt@cirt.me
Secondary method is by telephone and CIRT.ME can be reached at +382 20 247 863
Working hours from Monday to Friday (07:00h-15:00h)

3. Team charter

3.1.Mission:

The mission of the CIRT.ME is to achieve a high common level of cybersecurity across the conutry in cooperation with the other key entities.
CIRT.ME is in charge for handling, coordination and prevention of cyber security incident at the national level.

CIRT performs the function of protection against security incidents on the Internet and other risks related to the information security of its users. CIRT represents the point of contact at the national level for all computer security incidents in which one of the parties to the incident is located in Montenegro.

3.2.Constituents:

CIRT.ME is the Montenegrin CIRT and coordinates prevention and protection from security risks in ICT systems on the national level, advises and raises cyber security awareness for public institutions, government, private companies and for citizens.

3.3.Sponsorship and/or affiliation:

CIRT.ME is established in 2012 as part of a joint project of the Government of Montenegro and the International Telecommunication Union (ITU). Since November 2020 CIRT.ME operates within the National Security Authority.
CIRT is a member of the folowwing organizations:

- FIRST (Forum of Incident Response Teams) - https://www.first.org/members/teams/cirt-me
- TF-CSIRT (listed) (Task Force on Cyber Security Incident Response Teams) - https://www.trusted-introducer.org/directory/teams/cirtme.html

3.4.Authority:

CIRT.ME was established in accordance with the Law on Information Security and Data Secrecy Law. CIRT.ME is responsible for responding to computer security incidents in the cyber space of Montenegro. One of its objectives is to maintain active cooperation with all key cyber security institutions, local CIRTs (point of contact) and other stakeholders in the field of network and information/cyber security.

4. Policies

4.1.Types of Incidents:

CSEC CSIRT will respond to all reported incidents. Level of support provided will be factored by severity of incident, type of constituency, scope of incident and available CIRT.ME resources.

4.2.Cooperation, Interaction and Disclosure of Information:

Identifiable data will be adequately protected and will not be publicly published .
All information shared by CIRT.ME will be shared by using TLP 2 protocol. More information about TLP 2 protocol and its usage can be found at www.gov.me/cirt/tlp2
CIRT.ME may share statistical information about cybersecurity incidents.

4.3.Communication and Authentication:

Email with PGP should be used for encrypted communication of sensitive information. Email without PGP should be used only for non-sensitive information sharing.
Phone communication is considered safe enough for communication.

5. Services

5.1.Incident Response:

This service aims at providing information (e.g. on threat landscape, published vulnerabilities, new attack tools or technics, security/protection measures, etc.) needed to protect systems and networks. CIRT.ME will assist, in according to law of information security, within the constituency in handling the technical and organizational aspects of incidents.

5.2.Proactive services:

CIRT.ME coordinates and maintains following services to the extent possible depending on its resources:

- Publishing important security recommendations via web presentation, social networks or by email
- Training and seminars on cybersecurity related topics
- Consulting on cybersecurity resilience improvement

6. Incident reporting forms

Reports are normally sent to the e-mail address kontakt@cirt.me, but can also be reported via on-line form located at: https://www.gov.me/cirt/prijavi-incident

7. Disclaimer

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