monaco cyber sécurité

RFC 2350

Protéger. Auditer. Détecter. Réagir

SOMMAIRE

1. DOCUMENT INFORMATION

1.1 About this document

This document contains a description of CERT-MCS according to RFC 2350 specifications. It provides basic information about the CERT, how to contact the team, describes the roles and responsibilities and the service included in our offer.

1.2 Date of last update

Make sure you are using the latest version of this document.

Update history	Version	Comment
12/06/2022	V1	Creation of the document

Version 1.0 published on the 10/10/2023

1.3 Distribution list for notifications

The CERT-MCS does not use any distribution list to notify about changes made to this document.

If you have any question about this document, please contact us : cert@monacocyber.mc

1.4 Locations where this document may be found

This document can be found in our website: https://www.monacocyber.mc/medias_upload/moxie/cert_monacocyber_V1.pdf

1.5 Authenticating this document

This document has been signed with the CERT-MCS's PGP key. The signature is also provided on our web site, under:

https://www.monacocyber.mc/fr/r%C3%A9agir-47

1.6 Identification of this document

Title	cert_monacocyber_V1.pdf
Version	1.0
Date of publication	10/10/2023
Expiration	This document is valid until the publication of a new version.

2. CONTACT INFORMATION

2.1 Name of the team

Official team name: CERT Monaco Cyber Sécurité

Short name: CERT-MCS

2.2 Address

MONACO CYBER SECURITE

Le Copori, 9 avenue Albert II

98000 MONACO

2.3 Time zone

Central European [Summer] Time (CET/CEST), Europe/Paris (GMT+01, and GMT+02 on DST).

2.4 Telephone number

Hotline cover working hours only (duty office: 8h AM to 5h PM)

Phone: ++377 92002215

2.5 Fax number

Not Available

2.6 Other telecommunication

No other means of telecommunication

2.7 Electronic mail address

Email: cert@monacocyber.mc

2.8 Public key and encryption information

User ID: CERT-MCS

Fingerprint: F841 0A75 7DDC D445 709D CA4B A966 AF73 E449 25DB

KEY ID [LONG]: 0XA966AF73E44925DB

2.9 Team members

CERT MCS Contact	Position	Email
Sébastien MASSE	CEO of Monaco Cyber Sécurité	Sebastien.masse@monacocyber.mc
Anasse GHIRA	Responsible of SOC-MCS	anasse.ghira@monacocyber.mc

The list of all CERT-MCS members is not public.

2.10 Other information

Our website is available here: https://www.monacocyber.mc/

2.11 Point of customer contact

CERT-MCS prefers to receive incident reports via e-mail at cert@monacocyber.mc.

Please use our cryptographic key to ensure **integrity** and **confidentiality**. In case of emergency, please specify the **[URGENT]** tag in the subject field in your e-mail.

3. CHARTER

3.1 Mission statement

CERT-MCS is a private CERT team delivering Security services, mainly in the Principality of Monaco.

It has two main objectives:

- First, to assist its customers in implementing proactive measures to reduce the risks of computer security incidents.
- Second, to assist its customers in responding to such incidents against both intentional and opportunistic attacks that would hamper the integrity of their IT assets and harm their interests whenever they occur. The scope of CERT-MCS 's activities covers prevention, detection & analysis, response and recovery. CERT-MCS is in charge of digital forensics and incident response (DFIR) activities.

CERT-MCS will operate according to the following key values:

- CERT-MCS strives to act according to the highest standards of ethics, integrity, honesty and professionalism.
- CERT-MCS is committed to deliver a high-quality service to its constituency.
- CERT-MCS will ensure to respond to security incidents as efficiently as possible.
- CERT-MCS will ease the exchange of good practices between constituents and with peers, on a need-to-know basis.

3.2 Constituency

The CERT-MCS provides services to its customers which are located at Monaco and France.

CERT-MCS customers are found among:

- Private sector organizations
- Public sectors organizations
- Commercial organizations

CERT-MCS constituency also includes all the elements of Monaco Cyber Sécurité's Information System: its users, its systems, its applications, and its networks.

More information can be found on the Monaco Cyber Sécurité's website: https://www.monacocyber.mc/

3.3 Sponsoring and/ or Affiliation

CERT-MCS is part of Monaco Cyber Sécurité https://www.monacocyber.mc/ .

CERT-MCS maintains contact with various national and international CSIRT and CERT teams, on an as-needed basis.

3.4 Authority

For internal matters, CERT-MCS operates under the authority of the CEO of MCS.

For external incidents, CERT-MCS coordinates security incidents on behalf of its constituency, and only at its constituents' request. Consequently, CERT-MCS operates under the auspices of, and with authority delegated by its constituents.

CERT-MCS primarily acts as an advisor regarding local security teams and is expected to make operational recommendations. Therefore, CERT-MCS may not have any specific authority to require specific actions. The implementation of such recommendations is not a responsibility of CERT-MCS, but solely of those to whom the recommendations were made.

Generally, CERT-MCS expects to work co-operatively with its constituents' system administrators and users.

4. POLICIES

4.1 Types of incidents and level of support

CERT-MCS addresses all types of computer security incidents (cyber-attacks) which occur, or threaten to occur, in its constituency (see section 3.2).

The level of support given by MCS will vary depending on the type and severity of the incident or issue, the type of constituent, the importance of the impact on critical or essential infrastructure or services, and the CERT-MCS resources at the time.

Depending on the security incident's type, CERT-MCS will gradually roll out its services which include incident response and digital forensics.

4.2 Co-operation, interaction and disclosure of information

CERT-MCS considers operational co-ordination and information sharing between CERTs, CSIRTs, SOCs and similar bodies, as well as with other organizations that can assist in providing its services or offer benefits to CERT-MCS members, to be of paramount importance. Consequently, CERT-MCS exchanges all necessary information with affected parties, as well as with other CERTs, on a need-to-know basis. However, neither personal nor overhead data are exchanged unless explicitly authorized. Moreover, CERT-MCS will protect the privacy of its customers/constituents, and therefore (under normal circumstances) pass on information in an anonymized way only (unless other contractual agreements apply).

All incoming information is handled confidentially by CERT-MCS, regardless of its priority.

All sensible data (such as personal data, system configurations, known vulnerabilities with their locations) are stored in a secure environment, and are encrypted if they must be transmitted over unsecured environments as stated below.

CERT-MCS operates within the current French legal framework.

4.3 Communication and authentication

The preferred method of communication is email. For the exchange of sensitive information and authenticated communication CERT-MCS uses several encryption solutions. By default, all sensitive communication to CERT-MCS should be encrypted with our public PGP key detailed in section 2.8.

CERT-MCS protects sensitive information in accordance with relevant regulations and policies within Monaco/France and the EU.

CERT-MCS respects the sensitivity markings allocated by originators of information communicated to CERT-MCS ("originator control").

CERT-MCS supports the Traffic Light Protocol3 (TLP). Information that comes in with the tags TLP:WHITE, TLP:GREEN, TLP:AMBER or TLP:RED will be handled appropriately.

Communication security (which includes both encryption and authentication) is achieved using PGP primarily or any other agreed means, depending on the sensitivity level and context.

In CERT-MCS 's context of operations, the following communication security levels may be encountered in particular:

- Telephones will be considered sufficiently secure to be used (even unencrypted), given the types of information that CERT-MCS deals with.
- Unencrypted email will not be considered "secure" but will be sufficient for the transmission of low-sensitivity data.
- If it is necessary to send highly sensitive data by email, encryption (preferably PGP) will be used (see section 2.8). Network file transfers will be considered in the same way as emails for these purposes: sensitive data should be encrypted for transmission.

5. SERVICES

5.1 Digital Forensics and Incident Response (Triage, Coordination and Resolution)

CERT-MCS performs incident response for its constituency (as defined in 3.2).

CERT-MCS handles both the triage and coordination aspects. Incident resolution is left to the responsible administrators within the constituency. However, CERT-MCS will offer support and advice on request.

CERT-MCS will assist IT Security team 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:

- Incident Triage:
  - by investigating whether an incident occurred
  - by determining the extent of the incident
- Incident Coordination:
  - by determining the initial cause of the incident (exploited vulnerability)
  - by performing Digital Forensics whenever necessary (including hard drive and memory forensics)
  - by facilitating contact with Security Contacts and/or appropriate law enforcement officials, if necessary
  - by making reports to other CERTs (if applicable)
- Incident Resolution:
  - by fixing the vulnerability
  - by protecting the system from the effects of the incidentby evaluating whether certain actions are likely to reap results in proportion to their cost and risk

by gathering evidence where criminal proceedings or disciplinary measures are envisagedby collecting statistics on incidents that occur within or involve the constituency

CERT-MCS's incident response services try to cover the "6 steps": preparation, identification, containment, eradication, recovery, and lessons to be learned.

Please remember that the amount of assistance available from CERT-MCS will vary according to the parameters described in section 4.1.

5.2 Proactive activities

CERT-MCS develops in-house security tools for its own use, in order to improve its services and support its activities where necessary. Even though these security tools are used to provide benefits to CERT-MCS's constituency, they are not to be shared or used, neither by members of its constituency nor by members of the larger CERT, CSIRT and SOC communities.

6. INCIDENT REPORTING FORMS

No local form has been developed for reporting incidents to CERT-MCS.

In case of emergency or crisis, please provide at least the following information:

- Contact information, including electronic mail address and telephone number
- Date and time when the incident started
- Date and time when the incident was detected
- Incident description
- Affected assets, impact
- Actions taken so far

7. DISCLAIMERS

While every precaution is taken in the preparation of information, notifications and alerts, CERT-MCS assumes no responsibility for errors or omissions, or for damages resulting from the use of information contained in such documents, notifications or alerts.