CERT-MC
RFC 2350

Version : 1.8
Date : 03/07/2020

24, rue du Gabian
98000 MONACO
Tél. : (+377) 98 98 93 93
AMSN_contact@gouv.mc

Index

1- Document information

This document contains a description of CERT-MC in according to RFC 2350. It provides basic information related to the CERT-MC, the way it is operated and how it can be contacted. It also defines its roles and responsibilities, as well as the services offered to its constituency, which is defined in 3.2-.

1.1- Date of last update

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

Update History

Date	Version	Updates
07/04/2017	1.0	Document creation and review
18/07/2017	1.1	fax number added
17/10/2017	1.2	Alternate contact modes and links
19/12/2017	1.3	New PGP key added
26/12/2017	1.4	RFC updated to include the CERT-MC acronym
15/01/2018	1.5	URL for CERT-MC changed on AMSN's website
21/05/2019	1.6	Phone number changed.
27/06/2019	1.7	IP ranges and AS numbers under responsibility of CERT-MC added.

1.2- Distribution list for notifications

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

1.3- Locations where this document may be found

At any time, the current version this document is available from our website:

- **http://amsn.gouv.mc/CERT-MC/**

1.4- Authenticating this document

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

- **http://amsn.gouv.mc/CERT-MC/**

2- Contact information

2.1- Name of the team

Monaco government CERT

Short name: **CERT-MC**

2.2- Address

AGENCE MONEGASQUE DE SECURITE NUMERIQUE (AMSN) - CERT-MC

MONACO CYBER SECURITY AGENCY

24 rue du gabian

98000 Monaco

2.3- Time Zone

Central European Time

- GMT+0200 summer time (April to October)
- GMT+0100 winter time (November to march)

2.4- Telephone number

Secretariat: (+377) 98.98.93.93

Hotline covers working hours only.

2.5- Facsimile Number

Facsimile: (+377) 99 90 33 49 (please note this is ***not*** a secure fax).

2.6- Other Telecommunication

CERT-MC website: **https://amsn.gouv.mc/CERT-MC**

A static form for reporting incidents is available for download on CERT-MC's website.

2.7- Electronic mail address

CERT-MC uses two electronic mail addresses for distinct usages:

- **amsn_contact@gouv.mc** : general information or contact.
- **cert-mc@gouv.mc** : incident report.

Those email aliases relay mail to the human(s) on duty for the CERT-MC.

The general contact email should ***not*** be used to communicate with CERT-MC with regards to security incidents. Please use dedicated email instead: **cert-mc@gouv.mc**

For better handling, email should be given preference over fax/phone for reporting an incident to CERT-MC.

2.8- PUBLIC KEYS AND ENCRYPTION INFORMATION

CERT-MC uses a PGP key whose KeyID and Key Fingerprint are indicated here below:

- **Public key:** available on http://amsn.gouv.mc/CERT-MC/
- **Key ID:** 0x 5358CD2C
- **Key Fingerprint:** 0E7F 1AB1 52D2 76AA 7FC2 1184 231A E690 5358 CD2C

This key has also been made available for download on main GPG key servers.

2.9- TEAM MEMBERS

CERT-MC is operated by a team of security and forensic specialists from the government of the Principality of Monaco. The list of the staff members is not made available publicly.

Full identity of team members is disclosed on a need to know basis. For instance CERT-MC's members will communicate their full identities to third parties during resolution of incidents, once a trustful relationship has been established.

2.10- OTHER INFORMATION

Days/Hours of operation: 08:30 to 18:30 Monday to Friday.

2.11- POINTS OF CUSTOMER CONTACT

The preferred method for contacting CERT-MC is via electronic mail. This is even more applicable when it comes to urgent communication.

E-mail sent to CERT-MC's address will be automatically forwarded to the appropriate person on duty, immediately. If you require urgent assistance, put "urgent" in your subject line.

For reporting sensitive information, we strongly encourage our contacts to use PGP encryption (our PGP public key is available, section 2.8-).

Alternate incident reporting can be done via telephone or facsimile but is ***not*** recommended.

If possible, when submitting your report, use the form mentioned in section 6-. Handling of your report will be eased and CERT-MC will respond quicker.

Additional information can be found on our website: **http://amsn.gouv.mc/CERT-MC**.

3- Charter

3.1- MISSION STATEMENT

The purpose of CERT-MC is to coordinate cyber security efforts and incident response at national level in Monaco. More specifically, the missions of CERT-MC are listed here below:

- Anticipating, detecting, mitigating and resolving information cyber security incident.
- Addressing crisis situations caused by information security incident.
- Representing principality of Monaco within international committees involved in the fields of information security and incident response.
- Raising awareness and encouraging public services and strategic infrastructure operators to comply with good practices and requirements in terms of information security.
- Assessing current status of strategic infrastructure operators with regards to information security.

3.2- CONSTITUENCY

The constituency of CERT-MC is composed of:

- All government departments and public institutions.
- Strategic infrastructure operators.

In addition, CERT-MC also takes care of security incidents on the following perimeter:

- authoritative DNS for Monaco (nic.mc)
- all *.mc domain names

- ASN 6758, ASN 8799 : Monaco Telecom
  - 213.133.72.0/21 A7-interactive
  - 195.78.11.0/24 Monaco Telecom
  - 195.78.0.0/24 Monaco Telecom
  - 195.20.192.0/24 Gale Force
  - 188.191.136.0/21 A7-interactive
  - 185.47.116.0/22 A7-Test1-Net
  - 185.162.120.0/22 A7-Test1-Net
  - 185.250.6.0/24 Monaco Telecom
  - 185.250.4.0/24 Monaco Telecom
  - 176.114.96.0/20 A7-Test1-Net
  - 91.199.109.0/24 Single Buoy Moorings
  - 88.209.64.0/24 Monaco Telecom
  - 88.209.101.0/24 Monaco Telecom
  - 87.254.224.0/24 Monaco Telecom
  - 87.254.234.0/24 Monaco Telecom
  - 82.113.0.0/24 Monaco Telecom
  - 82.113.24.0/24 Monaco Telecom.

  - 80.94.99.0/24
  - 80.94.96.0/24
  -
- ASN 12463 : S.A. des bains de Mer et du Cercle des Etrangers à Monaco
  - 213.215.38.0/24
- ASN 48996 : Centre Hospitalier Princesse Grace
  - 37.44.224.0/22
- IP range : 149.5.230.0/24
- IP range: 85.118.63.160/27

3.3- SPONSORING AND/OR AFFILIATION

Funding of CERT-MC is provided by the government of Principality of Monaco, exclusively.

3.4- AUTHORITY

CERT-MC operates under the auspices of, and with authority delegated by sovereign ordinance 5664 dated the 23th of December 2015 and is operated by Monegasque Agency for Information Security (AMSN). The ordinance clearly defines the role of this entity, which has been placed under the authority of the Minister of State[1].

All constituents of CERT-MC have to report security incidents impacting their information system to CERT-MC.

Constituents from government departments and public institutions also have to follow CERT-MC's guidance in terms of information security.

The CERT-MC expects to work cooperatively with system administrators and users. However, should circumstances warrant it, the CERT-MC will appeal to IT department of third parties to exert its authority, direct or indirect, as necessary.

As far as strategic infrastructure operators, including ISPs and hosting providers, are concerned, with regards to the part of their information system used to operate the critical part of their activity, they are bound to follow CERT-MC's guidance, legal requirements and compulsory requirements.

Although CERT-MC does not have a direct authority on all of their information system, strategic infrastructure operators are also strongly encouraged to comply with the general guidelines issued by CERT-MC for the rest of their infrastructure.

4- Policies

4.1- TYPES OF INCIDENTS AND LEVEL OF SUPPORT

CERT-MC will provide support to its constituency only. Other third parties won't be supported.

CERT-MC is authorized to address all types of computer security incidents which occur, or threaten to occur, in our constituency networks (section 3.2-).

The level of support given by CERT-MC 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 our resources at the time the incident is handled by our team. During working hours, an acknowledgement will be sent within one hour.

Types of incidents will be prioritized according to their apparent severity and extent, assessed on a case-by-case basis.

Note that no direct support will be given to end users; they are expected to contact their system administrator, network administrator, or department head for assistance. The CERT-MC will support the latter people, belonging to its constituency only.

CERT-MC 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 by attackers.

4.2- CO-OPERATION, INTERACTION AND DISCLOSURE OF INFORMATION

CERT-MC cooperates with other CSIRTs and CERTs all around the world. It also exchanges all necessary information with appropriate organizations in the field of cyber incident response and/or information security.

These information may be related to critical vulnerabilities and/or security incidents, possibly impacting members of CERT-MC's constituency.

CERT-MC treats all submitted information as confidential per default, and will only forward it to concerned parties in order to resolve specific incidents when consent is implicit or expressly given. Therefore, appropriate measures will be taken to protect the identity of members of our constituency, members of neighboring sites, and privacy of reporters. For instance, information might be passed to third parties in an anonymized form.

Anytime where sensitive data need to be sent through insecure networks, information will be encrypted prior to transmission.

With regards to non-sensitive information, CERT-MC will share freely when it assists others in resolving or preventing security incidents.

CERT-MC supports TLP (Traffic Light Protocol[2]), and will categorize information before sharing with third parties. We will treat information accordingly if this categorization is included with the incoming information.

CERT-MC is not the national contact point for law enforcement authorities in the scope of Budapest convention on cybercrime (23/12/2001).

CERT-MC is the contact point for other CSIRTs/CERTs regarding cyber security incidents occurring in Monaco, or involving our constituents.

4.3- COMMUNICATION AND AUTHENTICATION

The preferred method for contacting CERT-MC is via electronic mail.

For regular exchange of information (containing no sensitive data), CERT-MC may use conventional means of communication like unencrypted e-mail, telephone, or facsimile.

In order to transmit sensitive or confidential information, PGP-encrypted e-mail should be used. Our constituents may also use ZED! Containers[3] further to agreement

Where it is necessary to establish trust, for example before relying on information given to the CERT-MC, or before disclosing confidential information, the identity and "bona fides" of the other party will be ascertained to a reasonable degree of trust.

This can be achieved also either through existing webs of trust (e.g. FIRST, TF-CSIRT, trusted third party) or by other methods like face-to-face meeting if necessary.

5- Services

5.1- INCIDENT RESPONSE

To make use of CERT-MC's incident response services, please send e-mail as per section 2.11- above. Please remember that the amount of assistance available will vary according to the parameters described in section 4.1- and 4.2-

5.1.1- Incident triage

- Investigating whether indeed an incident occurred.
- Determining the extent of the incident.
- Assessing and prioritizing the incident.

5.1.2- Incident coordination

- Determining the initial cause of the incident (vulnerability exploited).
- Facilitating contact with other parties which may be involved.
- Facilitating contact with the constituency and/or appropriate law enforcement officials, if applicable.
- Coordinating response to DDoS incidents (As there is only one ISP in Monaco, DDoS incidents must be coordinated at national level).
- Making reports to other CSIRTs and/or CERTs.
- Warning other constituents about newly identified vulnerabilities or methodologies, where applicable.

5.1.3- Incident resolution

- Advising local security teams on appropriate actions.
- Facilitating contact and coordinating actions where constituents need to call on private incident response providers or other security companies.
- Providing technical assistance to constituents.

Optionally, depending on its resources:

- Helping constituents to remove the vulnerabilities and the causes of incidents.
- Helping constituents to return back to the initial situation before the incident occurred.
- Helping constituents to collect evidence where criminal prosecution is contemplated.

5.2- PROACTIVE ACTIVITIES

The CERT-MC coordinates and maintains the following services to the extent possible depending on the context, and will try to gradually provide new services such as:

- Publishing announcements relating to serious security threats and new vulnerabilities.
- Advising its constituency on security solutions and architecture designs.
- Establishing statistics regarding incidents addressed by CERT-MC.

Optionally, depending on its resources:

- Monitoring current and emerging trends in cybersecurity.
- Raising awareness amongst its constituency.
- Providing security audits and penetration tests to its constituency.
- Collecting contact information and maintaining a directory of local security teams for internal use.

6- Incident reporting forms

A standard incident reporting form is available on CERT-MC's website at:

- **http://amsn.gouv.mc/CERT-MC/**

Whenever possible, please use this form to report incidents to CERT-MC.

If the sensitive information need to be protected, our PGP key is also available to encrypt the completed pdf file prior to sending it. For this purpose, our constituents may also use a ZED! Container, further to agreement.

7- Disclaimers

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

---

[1] http://journaldemonaco.gouv.mc/content/download/148384/3508834/file/JO_2015_J_8257.pdf

[2] http://www.first.org/tlp

[3] https://primx.eu/zed.aspx