



CERT-MC

RFC 2350

Version : 2.0
Date : 23/02/2022



Index

1- Document information	4
1.1- Date of last update	4
1.2- Distribution list for notifications	4
1.3- Locations where this document may be found	4
1.4- Authenticating this document	4
2- Contact information	5
2.1- Name of the team	5
2.2- Address	5
2.3- Time Zone	5
2.4- Telephone number	5
2.5- Facsimile Number	5
2.6- Other Telecommunication	5
2.7- Electronic mail address	5
2.8- Public keys and encryption information	6
2.9- Team members	6
2.10- Other information	6
2.11- Points of customer contact	6
3- Charter	7
3.1- Mission statement	7
3.2- Constituency	7
3.3- Sponsoring and/or affiliation	8
3.4- Authority	8
4- Policies	9
4.1- Types of incidents and level of support	9
4.2- Co-operation, interaction and disclosure of information	9
4.3- Communication and authentication	10
5- Services	11
5.1- Information Security Event Management (SOC services)	11
5.1.1- Monitoring and detection	11
5.1.2- Event analysis	11
5.2- Information Security Incident Management (CSIRT services)	11



5.2.1- Information security incident report acceptance.....	11
5.2.2- Information security incident analysis	12
5.2.3- Artifact and Forensic Evidence Analysis	12
5.2.4- Mitigation and Recovery.....	12
5.2.5- Information Security Incident Coordination	13
5.2.6- Crisis Management Support.....	13
5.3- Vulnerability Management (CSIRT services).....	13
5.3.1- Vulnerability Discovery/Research	13
5.3.2- Vulnerability Report Intake.....	13
5.3.3- Vulnerability Analysis	14
5.3.4- Vulnerability Coordination.....	14
5.3.5- Vulnerability Disclosure	14
5.3.6- Vulnerability Response	14
5.4- Situational Awareness	15
5.4.1- Data Acquisition.....	15
5.4.2- Analysis and Synthesis	15
5.4.3- Communication.....	15
5.5- Knowledge Transfer (CSIRT services).....	15
5.5.1- Awareness Building.....	15
5.5.2- Training and Education.....	16
5.5.3- Exercises	16
5.5.4- Technical and Policy Advisory	16
6- Incident reporting forms.....	18
7- Disclaimers.....	19



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 operates 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.
03/07/2020	1.8	Fax number changed
29/10/2021	1.9	Extended hours of operation
23/02/2022	2.0	Provided services updated according to CSIRT framework v2.1

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

Official team name: **CERT Monaco**

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

SOC: (+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: 07:30 to 21:30 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 (AMS). The ordinance clearly defines the role of this entity, which has been placed under the authority of the Minister of State¹.

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- Politiques

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.

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 Protocol²), 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.

CERT-MC is the national coordination center.

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! Containers³, Citadel Team, or Cryptobox 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.

An incident report form is available for download on CERT-MC website for critical infrastructure operators : <https://amsn.gouv.mc/CERT-MC/>



5- Services

5.1- INFORMATION SECURITY EVENT MANAGEMENT (SOC SERVICES)

Information security event management service is operated by the Security Operations Center of CERT-MC. This service is provided to CERT-MC constituency.

5.1.1- Monitoring and detection

Purpose: Implement automated, continuous processing of a wide variety of information security event sources and contextual data in order to identify potential information security incidents, such as attacks, intrusions, data breaches or security policy violations.

CERT-MC provides non-exhaustively the following functions:

- Log and sensor management
- Detection use case management
- Contextual data management

CERT-MC manages and operates sensors on networks pertaining to its constituency. It also correlates detected events with centrally collected logs, in order to assess the trustworthiness of detected anomalies.

For this purpose, CERT-MC defines use cases that help detecting security threats.

5.1.2- Event analysis

Purpose: Triage detected potential information security incidents and their qualification as information security incidents for escalation to the Information Security Incident Management service area or as false alarms

CERT-MC provides non-exhaustively the following functions:

- Correlation
- Qualification

Triage of the detected events is performed through information aggregation, correlation, and also enrichment from threat intelligence databases or services. The whole process is achieved with the help of a SIEM framework.

5.2- INFORMATION SECURITY INCIDENT MANAGEMENT (CSIRT SERVICES)

The following services are covered by CERT-MC incident response team (CSIRT) :

5.2.1- Information security incident report acceptance

Purpose: Receive and process reports of potential information security incidents from constituents, from Information Security Event Management services or third parties.

CERT-MC provides non-exhaustively the following functions:

- Information Security Incident Report Receipt



- Information Security Incident Triage and Processing

Internally within CERT-MC, once a verified security event has been qualified as a security incident during the monitoring and detection phase, this incident is escalated from SOC to CSIRT for follow-up.

CERT-MC also accepts reports from its constituents, partners, and other third parties.

To benefit from 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-

CERT-MC manually acknowledges and sends a receipt to all incident reports submitted by email, as soon as it starts processing the report.

5.2.2- Information security incident analysis

Purpose: Analyze and gain an understanding of a confirmed information security incident.

CERT-MC provides non-exhaustively the following functions:

- Information security incident triage (prioritization and categorization)
- Information collection
- Detailed analysis coordination
- Information security incident root cause analysis
- Cross-incident correlation

5.2.3- Artifact and Forensic Evidence Analysis

Purpose: Analyze and gain an understanding of artefacts related to a confirmed information security incident, taking into consideration the need to preserve forensic evidence.

CERT-MC provides non-exhaustively the following functions:

- Media or surface analysis
- Reverse engineering
- Runtime and/or dynamic analysis
- Comparative analysis

5.2.4- Mitigation and Recovery

Purpose: Contain the information security incident as much as possible to limit the number of victims, reduce the loss and to recover from damage, avoid further attacks and further losses by removing exploited vulnerabilities or weaknesses, and improve overall cyber security.

CERT-MC provides non-exhaustively the following functions:

- Response plan establishment
- Ad hoc measures and containment
- Systems restoration
- Other information security entities support



5.2.5- Information Security Incident Coordination

Purpose: Ensure timely notifications and accurate information distribution; keep the information flow and track the status of activities of entities that are either tasked or requested to participate in responding to the information security incident; and make sure the response plan is carried out and deviations caused by both delays or new information are managed accordingly.

CERT-MC provides non-exhaustively the following functions:

- Communication
- Notification distribution
- Relevant information distribution
- Activities coordination
- Reporting

5.2.6- Crisis Management Support

Purpose: Provide expertise and contacts to other security experts, CSIRTs, and CSIRT communities in order to help mitigate the crisis.

CERT-MC provides non-exhaustively the following functions:

- Information distribution to constituents
- Information security status reporting

5.3- VULNERABILITY MANAGEMENT (CSIRT SERVICES)

5.3.1- Vulnerability Discovery/Research

Purpose: Find, learn of, or search for new (previously unknown) vulnerabilities; vulnerabilities can be discovered by members of the vulnerability management service area or through other related CSIRT activities

CERT-MC provides non-exhaustively the following functions:

- Incident response vulnerability discovery
- Public source vulnerability discovery

CERT-MC **does not** conduct research activities aiming at identifying not previously known vulnerabilities. It mostly relies on external sources, or reports submitted by third parties to learn about vulnerabilities.

In the scope of incident response operations, it can also investigate on exploited vulnerabilities to gain further understanding of the methodology used by attackers.

5.3.2- Vulnerability Report Intake

Purpose: Receive and process vulnerability information reported from constituents or third parties.

CERT-MC provides non-exhaustively the following functions:

- Vulnerability report receipt



- Vulnerability report triage and processing

To report a vulnerability to CERT-MC, please send e-mail as per section 2.11- above.

CERT-MC manually sends a receipt to any vulnerability report submitted by email, as soon as it starts processing the report.

5.3.3- Vulnerability Analysis

Purpose: Analyze and gain understanding of a confirmed vulnerability.

CERT-MC provides non-exhaustively the following functions:

- Vulnerability triage (validation and categorization)
- Vulnerability root cause analysis
- Vulnerability remediation development

5.3.4- Vulnerability Coordination

Purpose: Exchange information and coordinate the activities with participants involved in a coordinated vulnerability disclosure (CVD) process.

CERT-MC provides non-exhaustively the following functions:

- Vulnerability notification/reporting

If a product or an equipment affected by a non-referenced vulnerability is reported to CERT-MC, vulnerability management service privately notifies the vendor on a need to know basis, via secure communication, and works with any relevant third party or PSIRT to help solving this vulnerability.

5.3.5- Vulnerability Disclosure

Purpose: Disseminate information about known vulnerabilities to constituents so that they can act upon that information to prevent, detect, and remediate/mitigate known vulnerabilities.

CERT-MC provides non-exhaustively the following functions:

- Vulnerability disclosure policy and infrastructure maintenance (*currently being drafted*)
- Vulnerability announcements/communication/dissemination
- Post-vulnerability disclosure feedback

In addition, CERT-MC informs any of its constituents as soon as CERT-MC is aware that a specific vulnerability has been detected on the constituent's network.

5.3.6- Vulnerability Response

Purpose: Actively take information about known vulnerabilities and act upon that information to prevent, detect, and remediate/mitigate those vulnerabilities.

CERT-MC provides non-exhaustively the following functions:

- Vulnerability detection / scanning
- Vulnerability remediation



In order to perform vulnerability response, CERT-MC gathers information from internal teams within its constituency, or collect data from databases provided by third parties.

CERT-MC provides support to its constituents in order to mitigate or remediate vulnerabilities found on their networks.

5.4- SITUATIONAL AWARENESS

5.4.1- Data Acquisition

Purpose: Collect data that will help increase visibility as to what internal and external activities are occurring that may affect the constituency's security posture.

CERT-MC provides non-exhaustively the following functions:

- Policy aggregation, distillation, and guidance
- Asset mappings of assets to functions, roles, actions, and key risks
- Collection
- Data processing and preparation

5.4.2- Analysis and Synthesis

Purpose: Assess when the situation does not match with expectations (e.g., when specific assets may be about to experience a harmful event).

CERT-MC provides non-exhaustively the following functions:

- Projection and inference
- Event detection (through alerting and/or hunting)
- Situational impact

5.4.3- Communication

Purpose: Notify constituents or others in the security community about changes in risks to the situational picture.

CERT-MC provides non-exhaustively the following functions:

- Internal and external communication
- Reporting and recommendations
- Implementation
- Dissemination / integration / information sharing
- Management of information sharing

5.5- KNOWLEDGE TRANSFER (CSIRT SERVICES)

5.5.1- Awareness Building

Purpose: Increase the overall security posture of the constituency and help its members to detect, prevent, and recover from incidents; ensure that constituents are better prepared and educated.



CERT-MC provides non-exhaustively the following functions:

- Research and information aggregation
- Report and awareness materials development
- Information dissemination
- Outreach

CERT-MC collects, aggregates, and disseminates information regarding security threats to its constituency, on a daily basis. It also produces non-technical and high-level weekly digests.

5.5.2- Training and Education

Purpose: Provide training and education to a CSIRT constituency (which may include organizational and CSIRT staff) on topics related to cybersecurity, information assurance and incident management.

CERT-MC provides non-exhaustively the following functions:

- Knowledge, skill, and ability requirements gathering
- Educational and training materials development
- Content delivery
- Mentoring
- CSIRT staff professional development

CERT-MC also shares feedbacks on solved security incidents it had to take care of. Those education sessions improve the skills of security teams amongst its constituency.

5.5.3- Exercises

Purpose: Conduct exercises to assess and improve the effectiveness and efficiency of cybersecurity services and functions.

CERT-MC provides non-exhaustively the following functions:

- Requirements analysis
- Format and environment selection (environment development performed by third party)
- Scenario selection (scenario development performed by third party)
- Exercises execution
- Exercise outcome review

CERT-MC organizes cyber security exercises (CTF), with the help of third party companies, to assess and improve incident response capabilities of its constituents.

5.5.4- Technical and Policy Advisory

Purpose: Ensure the constituency's policies and procedures include appropriate incident management considerations and, ultimately, enable the constituency to better manage risks and threats, as well as enabling the CSIRT to be more effective.

CERT-MC provides non-exhaustively the following functions:

- Business continuity and disaster recovery planning support
- Policy support



- Technical advice

CERT-MC has clearly defined guidelines and policies in terms of security posture for its constituency. CERT-MC provides technical advisory to its stakeholders and constantly helps them cope with the guidelines.



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 sensitive information must 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, Citadel Team or Cryptobox 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>