May, 22nd 2022

RFC 2350 DESCRIPTION

for

MARITIME COMPUTER EMERGENCY RESPONSE TEAM (M-CERT)

TLP:WHITE

1. DOCUMENT INFORMATION

This document contains a description of the French Maritime Computer Emergency Response Team, hereafter also shortened as Maritime CERT or M-CERT, in accordance with the RFC 2350 document[1].

It provides information about the M-CERT, its channels of communication, its roles, responsibilities and the services offered.

1.1 – DATE OF LAST UPDATE

This is version 1.60, published on May, 22nd 2022.

1.2 – DISTRIBUTION LIST FOR NOTIFICATIONS

M-CERT does not use any distribution list to notify about changes in this document.

Please send questions about updates to M-CERT's team email address: <contact(at)m-cert.fr>.

1.3 – LOCATIONS WHERE THIS DOCUMENT MAY BE FOUND

The current version of this Computer Security Incident Response Team (CSIRT) description document is available from M-CERT's website at the following URL: https://www.m-cert.fr/rfc/M-CERT_RFC_2350_v1.60.pdf.

1.4 – AUTHENTICATING THIS DOCUMENT

This document has been signed with M-CERT's PGP key.

The PGP public key is available on the M-CERT's website https://www.m-cert.fr/key/M-CERT_public_key.asc.

The signature is made available on the M-CERT's website at: https://www.m-cert.fr/rfc/M-CERT_RFC_2350_v1.60.pdf.sig.

1.5 – DOCUMENT IDENTIFICATION

- Title: "M-CERT_RFC2350_v1.60"
- Version: 1.60
- Document Date: 2022-05-22
- SHA 256: see https://www.m-cert.fr/rfc/M-CERT_RFC_2350_v1.60.pdf.sha256.txt
- Expiration: this document is valid until superseded by a later version

Please make sure you are using the latest version.

1 RFC 2350 is an IETF Best Current Practice available at: www.ietf.org/rfc/rfc2350.txt

2. CONTACT INFORMATION

2.1 – NAME OF THE TEAM

- Official name: Maritime Computer Emergency Response Team
- Short name: M-CERT

2.2 – ADDRESS

FRANCE CYBER MARITIME

M-CERT

Hôtel de métropole

24, rue Coat-ar-Guéven – CS 73826

29238 BREST CEDEX 2 – France

2.3 – TIME ZONE

GMT+1 (with Daylight Saving Time or Summer Time, which starts on the last Sunday in March and ends on the last Sunday in October). Also known as Central European Time (CET)/Central European Summer Time (CEST).

2.4 – TELEPHONE NUMBER

Main number (duty office): +33 (0) 257 520 987

2.5 – FACSIMILE NUMBER

None available.

2.6 – OTHER TELECOMMUNICATION

A Signal channel can also be established with the following mobile phone number: +33 (0) 782 290 175. M-CERT does not plan to use other messaging systems and will not respond to any other channel establishment request.

2.7 – ELECTRONIC MAIL ADDRESS

If you need to notify us about an information security incident or a cyber-threat targeting or involving the maritime or port sector, please contact us at: <contact(at)m-cert.fr>.

2.8 – PUBLIC KEYS AND OTHER ENCRYPTION INFORMATION

MCERT uses the following OpenPGP public key:

- User ID: Maritime CERT <contact(at)m-cert.fr>
- Fingerprint: 8A1E C5D2 B7C0 EFA4 9FFB 31FC 2485 CF71 E37B EBB7
- KeyID: 0x2485CF71

The public key and its signatures can be found at the usual large public key servers (such as pgp.mit.edu) and are also available on our website at: https://www.m-cert.fr/key/M-CERT_public_key.asc. Our current PGP-Key is also available under request by sending an email at <contact(at)m-cert.fr>.

The key shall be used whenever information must be sent to M-CERT in a secure manner.

Please use this key when you need to encrypt emails sent to M-CERT and sign your messages using your own key. It helps when your key can be checked upon for instance using the public key servers.

2.9 – Team Members

M-CERT team is composed of cyber security analysts or specialists, most of them with a significant maritime experience.

For privacy concerns, the names of the team members are not released publicly. The identity of the team members might be disclosed to our constituency on a case-by-case analysis, based on need-to-know restrictions.

Please contact directly M-CERT for more detailed information.

2.10 – Other Information

General information about M-CERT, as well as links to various recommended security resources can be found on our website at www.m-cert.fr.

M-CERT also owns a Twitter account (@M_CERT_FR) and a LinkedIn account (M-CERT). Those accounts are only meant to disseminate information from M-CERT and should not be used to send sensitive information to M-CERT.

2.11 – Point of Customer Contact

The preferred method for contacting M-CERT is via email at <contact(at)m-cert.fr>. If you require urgent assistance, please specify the [URGENT] tag in the subject field of your email. Please use our cryptographic key to ensure intergrity and confidentiality when sending any sensitive information to M-CERT.

If it is not possible (or not adviseable for security reasons) to use email, M-CERT can be contacted by telephone during regular office hours (see 2.4 and 2.6).

M-CERT's hours of operation are generally restricted to regular business hours (09:00-18:00, CET/CEST (DST), Monday to Friday).

M-CERT is closed on Saturdays and Sundays, as well as on French bank holidays.

3. CHARTER

3.1 – MISSION STATEMENT

M-CERT is a non-profit CSIRT for both public and private entities of the global maritime and port sector, in France and at an international level when needed.

The purpose of M-CERT are:

- First, to assist its constituency in implementing proactive measures to reduce the risks of computer security incidents;
- Second, to assist its constituency in responding to such incidents when they occur.

M-CERT missions cover prevention and incident management within the maritime and port sectors by:

- Helping to prevent security incidents by:
  - Improving cybersecurity awareness,
  - Promoting the implementation of necessary protection measures to enhance resilience,
  - Detecting vulnerabilities on networks and systems.
- Analyzing vulnerabilities, threats, attacks and risks with a sectoral perspective;
- Sharing information of interest for the sector:
  - By disseminating dedicated bulletins and Cyber Threat Intelligence on new cyber threats and attacks,
  - By broadcasting national and international security alerts and warnings.
- Managing cyber incidents by:
  - Organizing, coordinating, centralizing, collecting and identifying cyber incidents under both technical and organizational aspects,
  - Searching for trusted partners to support our constituency with incident response when necessary.
- Cooperating at regional, national, european and international levels with relevant maritime or cyber public and private entities, as well as other industrial sectors when needed, to build trusted networks on maritime cybersecurity.

3.2 – CONSTITUENCY

M-CERT is the CSIRT for the maritime sector in France, at a national and, if requested, at the european level. The primary constituency is composed of all french territories (DROM-COM included) supporting maritime and port operations, at large, at sea and ashore and cover:

- Stakeholders from public organizations;
- Operators and private companies;
- Other key players in the maritime and port sector.

M-CERT proposes both paid and open services to its constituency.

3.3 – Sponsoring / Affiliation

Sponsorship and Funding

M-CERT activities are funded and operated by the non-profit organization (known as "Loi 1901 association", in French) called "France Cyber Maritime". The organization's board (Steering Committee) leads and reviews the activities of M-CERT services.

M-CERT also benefits from coordination agreements on maritime cybersecurity signed between France Cyber Maritime and the French Navy and with the French Gendarmerie Maritime.

M-CERT has received an initial financial funding and support by the French National Cybersecurity Agency (Agence Nationale de Sécurité des Systèmes d'Information, ANSSI) and by the French Secretary for the Sea (Secrétariat Général de la Mer, SGMer).

Affiliation

At the international level, M-CERT plans to be a member of the FIRST organization (www.first.org).

At the european level, M-CERT plans to become an accredited member of the Trusted Introducer (www.trusted-introducer.org) and is willing to participate to the CSIRT Task Force (https://www.geant.org/People/Community_Programme/Task_Forces/Pages/TF-CSIRT.aspx), which promotes the collaboration between Computer Security Incident Response Teams (CSIRTs) in Europe.

At a domestic level, M-CERT is a member of the French CERTs group: InterCERT-France (www.cert.ssi.gouv.fr/csirt/intercert-fr/) and will work with other CSIRTs, either sectoral or regional when needed.

At the international, european and domestic levels, M-CERT aims to cooperate with maritime CSIRTs and other existings Security Operation Centers (SOCs), Information Sharing and Analysis Centers (ISACs), according to its needs and the information exchange culture that it values, but still respecting the need-to-know basis.

3.4 – Authority

The handling of maritime cyber security-related computer incidents in France is stated in the actual national regulation (www.sgdsn.gouv.fr/uploads/2018/08/20180627-instruction-interministerielle-nxx-230-surete-maritime-portuaire.pdf).

M-CERT services are performed by a technical team constituted of employees of the non-profit organization France Cyber Maritime. They expect to work cooperatively with network, system, IT and OT administrators.

4. POLICIES

4.1 – TYPES OF INCIDENTS AND LEVEL OF SUPPORT

M-CERT addresses all types of cyber security incidents which occur, or threaten to occur, in its constituency. We are setting a special attention to incidents relative to maritime and port assets: Information Technology (IT), Operational Technology (OT), Industrial Control Systems (OT), telecommunication systems, Position, Navigation, Time (PNT) systems, specific protocols, assets, individuals, threat actors, Tactics, Technics and Procedures, and vulnerabilities.

The level of support provided by M-CERT will vary, depending on:

- The type and severity of the incident or issue,
- The potential or assessed impact of the incident,
- The type of constituent,
- The size of the impacted user community affected,
- M-CERT's resources at the time.

Incidents will be prioritized according to their apparent severity and extent.

M-CERT's services include reactive and proactive services for the maritime and port sectors detailed in Section 5.

Note that a limited support will be given to end-users, depending on the situation. They are expected to contact at first their internal relevant correspondant (system/network administrator, department head) for assistance and advice. M-CERT will support the latter people.

At M-CERT, we understand that there exists great variation in the maturity and knowledge level of system or network administrators within the sector. While we will endeavor to present information and assistance at an appropriate level to each person, we cannot train system or network administrators on the fly, and we cannot perform system maintenance on their behalf. In most cases, we will provide them with pointers to the information needed to implement appropriate security measures.

M-CERT is committed to keeping its constituency community informed of potential vulnerabilities and, where possible, will inform this community of such vulnerabilities before they are actively exploited.

4.2 – CO-OPERATION, INTERACTION AND DISCLOSURE OF INFORMATION

There are legal and ethical restrictions on the flow of information being exchanged between cybersecurity actors such as CSIRTs, both for preventive and reactive actions.

However, in order to accomplish its mission and perform its services to prevent and react to cybersecurity incidents, the M-CERT needs to exchange information with its constituency, but also with other CERT/CSIRTs, SOCs or ISACs, as well as with affected parties' administrators.

Therefore, appropriate measures must be taken to protect personal, technical and contextual information. In this context, M-CERT's first priorities are to preserve:

- The level of confidentiality assigned to the information by its owner,
- The privacy of personal information.

Without agreement, any supplied information is, by default, kept confidential. General incident related information such as personal, technical or contextual data will not be disclosed by the M-CERT.

In case of a written agreement by the named parties, all necessary information exchanged with affected parties, as well as with other CSIRTs, SOCs, ISACs and M-CERT's constituency will be achieved on a need-to-know basis. Unless explicitly authorized, neither personal, technical or precise contextual data are exchanged: M-CERT will only relay specific and relevant technical extracts to its constituency and partners, and only if the corresponding data can prevent further incidents.

All information is passed depending on its classification and the need-to-know principle. M-CERT respects the Information Sharing Traffic Light Protocol (TLP). Information that comes with the tags WHITE, GREEN, AMBER or RED as described by the FIRST definitions at https://www.first.org/tlp/ will be handled appropriately.

M-CERT will never pass information to third parties out of its constituency, unless required by law or without a prior agreement of the information owner.

M-CERT handles and processes information in secured physical and technical environments, in accordance with the French state and EU regulations for the protection of information.

M-CERT operates within the current French legal framework. If needed, public authorities may engage the M-CERT on incidents affecting non-maritime sectors.

The M-CERT will not interact directly with the Press concerning any specific computer security incident, except to point them toward information already released to the general public. The above does not affect the ability of members of M-CERT to grand interviews on general computer or specific maritime and port cyber security topics.

4.3 – COMMUNICATION AND AUTHENTICATION

M-CERT protects sensitive information in accordance with relevant French and European regulations and policies within France and the EU. M-CERT also respects the sensitivity markings allocated by originators of information communicated to the M-CERT ("originator control").

M-CERT also recognizes and support the Traffic Light Protocol (see Section 4.2).

The preferred method of communication with M-CERT is email.

In M-CERT's context of operations and in view of the context and the types of information that M-CERT deals with, the following communication security levels may be encountered:

- For general non-sensitive or non-restricted communication and when both parties agree, unencrypted phone-call, video-conferencing, unencrypted email or postal service may be used. Unencrypted email is not considered particularly secure, but can be used for the transmission of low-sensitivity data;
- For communication security, which includes both encryption and authentication, M-CERT encourages the use of PGP signed emails to exchange sensitive data (such as personal data, system configurations, known vulnerabilities with their locations) over unsecure communication channels such as public email. By default, all sensitive communication to M-CERT should be encrypted with our public PGP key detailed in Section 2.8. Alternate encryption solutions are also available. Network file transfers are similar to email for these purposes, however sensitive data should also be encrypted in that case for transmission. If inappropriate to the other party, other means of communications may be used as well, e.g. symmetric encryption with a password key set beforehand.

4.4 – Vulnerability Disclosure Policy

This policy is applied by M-CERT when M-CERT is aware of a new security vulnerability that has not been disclosed publicly yet. This policy aims at ensuring security for M-CERT constituency and at enabling Vendors to quickly troubleshoot their security problems.

M-CERT is committed to providing assistance, within its capabilities, to act as a trusted contact between a Reporter (who discovered a new security vulnerability) and the Vendor of the solution affected by this vulnerability. As such, M-CERT acts as a Coordinator, as defined in the RFC Draft "Responsible Vulnerability Disclosure Process" (published by IETF in February 2002). It may also sometimes act as a Reporter. If M-CERT is unable to provide this coordination service, out of resource constraints, then, it will inform the impacted parties and offer them alternative solutions.

M-CERT undertakes to follow a grace period, which is generally of 90 days, before publishing its advisories. Thus, during the discovery process of a new vulnerability, M-CERT notifies the Vendor, letting him know that the information will be published, should no response be supplied by the end of the grace period. If the threat importance requires to shorten this delay, the various actors (specifically the Vendor) will be informed. This grace period only applies to new vulnerabilities, which means

vulnerabilities that have not already been published on a public forum (open mailing lists, public websites, etc...).

During this Vendor notification period, M-CERT undertakes to provide all necessary information to enable the Vendor to qualify the vulnerability: problem description, tested versions, code used and all technical information useful for the problem understanding. The notification is generally made by email and the notification date is recorded.

Unless the Reporter disagrees, M-CERT will indicate the Reporter’s name to the Vendor during the notification, and to M-CERT constituency when the advisory is released.

M-CERT policy will be enforced equally for all Editors.

However, in case of significant security risks, M-CERT reserves the right to publish the information before or after the grace period. This decision to publish or not an advisory will always take into account the interests in terms of security of the various actors. Whenever possible, M-CERT will propose a workaround to allow the users to protect themselves against the vulnerability exploitation.

5. SERVICES

M-CERT coordinates and maintains the following services tailored for the maritime and port sectors to the extent possible, depending on its resources and on the type of service (free/paid). More information can be obtained via email at <contact(at)m-cert.fr>. Information on these services is also vailable from M-CERT's website www.m-cert.fr.

5.1 – INCIDENT RESPONSE

To make use of M-CERT incident response services, please send e-mail as described in Section 2.11 above. Please remember that the amount of assistance available will vary according to the parameters in Section 4.1.

5.1.1 – INCIDENT MANAGEMENT

M-CERT aims at being the relevant point of contact for the maritime and port sector and at providing support to collect, identify, centralize and manage cyber incidents in accordance with laws and regulations that apply.

5.1.2 – INCIDENT RESPONSE COORDINATION

M-CERT aims at supporting the maritime sector in handling the technical and organizational aspects of incidents. In particular, M-CERT provides 2 major services in the field of Incident Response Coordination:

INCIDENT TRIAGE

The role of M-CERT for Incident Triage encompasses:

- The collection of information about the incident,
- The confirmation that the described event is currently a cyber security incident and is related to M-CERT's constituency,
- The determination of the severity level of the incident, based on its impact, its extent (number of affected users), and the type of service (coordination or escalation to other Third Parties) to be triggered.

INCIDENT COORDINATION

The role of M-CERT for Incident Coordination is:

- To categorize the incident related information with respect to the information disclosure policy,
- To determine the initial cause of the incident (e.g. vulnerability exploited…),
- To facilitate contact with appropriate law enforcement officials, other CSIRTs or companies specialized in incident resolution, if necessary,
- To provide anonymity to the Reporting entity who wants to contact involved Third Parties anonymously,
- To provide assistance, within its capabilities, to ease the sharing of information between the Reporting entity and the Third Parties,

- To collect or contribute to collect evidence of the incident,
- To support at its best the involved parties during the incident management process,
- To build and share lessons learned following a cyber security incident.

In addition, M-CERT will centralize collect statistics concerning processed incidents, and will notify the community as necessary to assist it in protecting against known attacks.

Incident resolution and recovery processes themselves, remain of the resposibility to the involved party, together with the partner they eventually choose to support them.

5.2 – Proactive Activities

M-CERT aims at improving maritime and port cyber security by providing its constituency with several proactive services to enhance awareness and prevent cyber security events.

Alerts and Warnings

In case of a specific event, such as an alert, an incident or a crisis, M-CERT disseminates information to its constituency and provides recommendations to tackle the issue. Such alerts and warnings may be passed on to other CERTs, CSIRTs, ISACs, SOCs and similar bodies if deemed necessary of useful for them to prevent further cyber attacks and on a need-to-know basis. Such information services are available via dedicated and closed mailing lists.

Announcements

M-CERT provides regular information on published vulnerabilities, new attack tools and security measures needed to protect its constituency's information systems by the publication of regular bulletins on maritime cybersecurity. M-CERT is not responsible for the implementation of its recommendations. Such alerts and warnings may be passed on to other CERTs, CSIRTs, ISACs, SOCs and similar bodies if deemed necessary of useful for them to prevent further cyber attacks and on a need-to-know basis. Such information services are available via dedicated and closed mailing lists.

Awareness and Dissemination

M-CERT aims at sharing its knowledge and experience to enhance awareness on maritime cyber security topics through dissemination, by its participation in research activities and projects, by the use of dedicated communication channels with Chief Security Officers (CSOs) and Chief Information Security Officers (CISOs), but also through its participation in cybersecurity and/or maritime and port events and conferences.

Cyber Threat Intelligence

M-CERT provides its constituency with regular information and analysis on the maritime and port cyber threat landscape. M-CERT also builds and shares artefacts, such as Indicators of Compromise (IoCs). Such alerts and warnings may be passed

on to other CERTs, CSIRTs, ISACs, SOCs and similar bodies if deemed necessary of useful for them to prevent further cyber attacks and on a need-to-know basis. Such information services are available via dedicated and closed mailing lists.

Passive Preventive Monitoring

M-CERT performs passive preventive monitoring actions on maritime and port assets to detect potential breaches or vulnerabilities and misconfigurations which may be leveraged during cyber attacks. When necessary, reports are sent to the concerned parties in due time, respecting legal frameworks and the sensitivity of the potential discovered vulnerabilities.

Research and Survey

M-CERT aims at conducting cyber security research, expertise and survey activities for the whole maritime and port sector to detect new vulnerabilities and enhance cybersecurity. M-CERT provides the “Advanced Database of Maritime cyber Incidents Released for Litterature” (ADMIRAL), available from https://gitlab.com/m-cert/admiral/, which tries to include all disclosed maritime cyber security incidents for research and education purposes.

Vulnerability Disclosure

In accordance with its Vulnerability Disclosure Policy in Section 4.4, M-CERT will act as a Coordinator, between a Reporter (organization or unit triggering the incident process) and Third Parties (stakeholders involved in the resolution of the incident or other CSIRTs).

Vulnerability Monitoring

When mandated by a constituency, M-CERT is able to watch available public announcements on vulnerabilities concerning specific software or hardware and alert the concerned party in case of discovery.

Many other services such as education, training, auditing, consulting, etc. are also available through the France Cyber Maritime non-profit organization. More information on France Cyber Maritime’s services is available on the organization’s website www.france-cyber-maritime.eu.

6. INCIDENT REPORTING FORMS

There are no local forms developed yet for reporting incidents to M-CERT. We strongly suggest to use the procedures detailed in Section 2.8 and Section 2.11 and to encrypt any private or confidential information.

Please make sure that your incident report contains at least the following information:

- Your contact and organizational information – name and organization name, email, full telephone number, and case type,
- Date and time when the incident started (including time zone),
- Date and time when the incident was detected (including time zone),
- Detailed description of the incident including:
    - Source/Destination IPs and/or Full Qualified Domain Name (FQDN),
    - Ports and protocols,
    - Relevant Indicators of Compromises (IoCs),
    - Excerpts of logging showing the incident activity,
    - Any scanning result by antivirus or alert from security device,
    - For GNSS and AIS spoofing or jamming: latitude, longitude, course, symptoms, duration, consequences
    - Full source of email in case of phishing incident (email headers, body and any attachment if possible and as permitted by the regulations, policies and legislation under which you operate),
    - Affected product with detailed version of software or hardware,
    - Affected assets and feared or actual operational, human, environmental or legal impacts,
    - Actions taken so far,
    - Expectations or priorities.
- Any other relevant information that could assist M-CERT in understanding the incident case type (files, printscreens, emails, architecture drawings, private IP addresses list, etc.).

7. DISCLAIMERS

While every precaution is and will be taken to prepare its information, notifications and alerts, M-CERT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.

If you notice any mistakes within this document, please email us. We will solve those issues as soon as possible.