CERT-XMCO profile

Established according to RFC-2350.

1. Document Information

This document contains a description of CERT-XMCO in according to RFC 2350. It provides basic information about the CERT-XMCO team, and the ways it can be contacted. It also describes its responsibilities and the services offered.

1.1 Date of Last Update

Version 2.0, created on 2026-01-01.

1.2 Distribution List for Notifications

There is no distribution list for notifications.

This document is kept up-to-date at the location specified in 1.3.

Updates are also reported to the Trusted Introducer publicly accessible directory (see https://www.trusted-introducer.org/trusted-introducer/directory)

Should you have any questions regarding updates, please contact the CERT-XMCO email address.

1.3 Locations where this Document may be Found

The current and latest version of this document is available from CERT-XMCO's website. Its URL is:

- https://www.xmco.fr/cert-xmco/profile-rfc2350

Please make sure you are using the latest version.

1.4 Authenticating this Document

This document has been signed with the CERT-XMCO's PGP key. The signature is available from CERT-XMCO's website. Its URL is:

- https://cert.xmco.fr/CERT-XMCO_rfc_2350.pdf.sig

See section 2.8 for more details.

1.5 Document Identification

- *Title*: CERT-XMCO RFC-2350
- *Version*: 2.0
- *Document Date*: 2026-01-01
- *Expiration*: this document is valid until superseded by a later version.

2. Contact Information

This section describes how to contact CERT-XMCO.

2.1 Name of the Team

- *Full name*: CERT-XMCO
- *Short name*: CERT-XMCO

CERT-XMCO is XMCO's commercial CERT/CSIRT team (Computer Emergency Response Team / Computer Security Incident Response Team).

2.2 Address

```
CERT-XMCO
18 rue Bayard, 75008 Paris
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 `CET` / `CEST`

2.4 Telephone Number

- +33 (0)1 47 34 30 38 (French business hours)

2.5 Facsimile Number

None available.

2.6 Other Telecommunication

- Twitter: `@certxmco`

2.7 Electronic Mail Address

If you need to notify us about an information security incident or a cyber-threat targeting or involving your company or XMCO, please contact us at cert@xmco.fr. This is a mail alias that relays mail to CERT-XMCO's analysts on duty.

2.8 Public Keys and Encryption Information

PGP/GnuPG is supported to secure communication.

Consequently, the CERT-XMCO has a PGP key (bound to the cert@xmco.fr mail address), whose ***KeyID*** is `CB73D838` and
whose ***Fingerprint*** is `2ED2 3D0D C312 C70B BB89  FEBA 7D0A 6D02 CB73 D838`.

- The current CERT-XMCO team-key can be found at https://www.xmco.fr/cert-xmco/CERT-XMCO.asc. The key can also be retrieved from the usual public key servers, such as https://keys.openpgp.org/.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: GPGTools - http://gpgtools.org

mQINBGoBjNkBEACl1UWAF8eJPJ3+anr9D7KLts4v/Pzs4svQ4CM1Ov8pyJIc8A1/
MkahrMngTb1zNexnzo1ymR54GGz1bTdf0MQjSNzGMmi9WpRFaiEqi/hFd0yDFwE1
L9n+WonjYYjv//qjpxYk70HcSHpouPptQHGhmjJGVamrhoWMuDHBlkONsyuDZlZp
pHqllULEpYDr/dhJwKVA8VOoaWwdSq4OVmAsuUvNiPyTTo2PYD37xOjivWchOYnW
9mMgd/Afi8AiZFr5F95813WF6mA/N3r3AdXdOoudictoVHkMCwNI5arS9S67TvXE
bzo80Wa8awJov9JNmcjA9quQvC5xF2E3nLRdcumivPnRfz1O4Z6kJ5b2bk5pGCFV
lQoOyEX25Pt2huG8nuxojwJHcfkR+lek8bjy8KPoo9wLKcXrr3EfhBfxHGpU13ik
SMuDSQjYPXZo24bNKTZ9R1VDh74kK8s4XtJiiKNZzLec64N3CJdn/PEEdub7bkpr
2FeWMyZAlduxK6Q3pYbeiZ0KXYs9ImowU4LrY2qrqkNXMQOXCXXvABsw3kK/YVBn
SI8Yxso+yxGrh4lZFlrLet39Z7AbVYnXEubkY1GGAxG9wsQhKUF6bxwZU1r2ptRJ
JVFdadLl5cWL7Q6YTi4ZJoNfVSU4ja9nLzu2J7difEXC6QEcVE24vlo7OQARAQAB
tDtDRVJULVhNQ08gKENlY2kgZXN0IGxhIGNsZSBncGcgZHUgQ0VSVC1YTUNPKSA8
Y2VydEB4bWNvLmZyPokCTgQTAQgAOBYhBC7SPQ3DEscLu4n+un0KbQLLc9g4BQJq
AYzZAhsDBQsJCAcCBhUKCQgLAgQWAgMBAh4BAheAAAoJEH0KbQLLc9g4MEMP/i7V
mhhix62Aon7h6DuRJesxydQEAC94V8RmSwsbskJw26jXUew7/9fqBBatqvtFJvXC
wxaLd+EYtO45hzn8+tlhtJqgxq/nF5JrNb1Jt9L1P2w2dSzAaZd8VgSekcJpuYTd
NdrKl7ilRvSQ+FuI52GlFDb0FZJUEbGNg6r2WBC7C/ag4DGMdiZl2w6MzbfbErue
dfszNgyFQ5iawa15kfl4IH3VAhydalLIVEOWANvx7SN9d9E7354Q1PaGKL0Jyx1P
B2mskjKxOb3EZrsbWg7m1VOZHq+v+CBzKRfcqSDTS0f1uKPHq5Rn1Mpwq/Pl1Dgy
X8Np+SDvLdaNiCKL/wV2pAqQJJDYjjHwgjjMdmyDfD0JPL+x0EyFDPEBD1XzNVYj
1oI4dZYmPhAhL9gK3DlrmBZG0fOjsGgOgKmnqtvS42SLWd3gy4gegjUzyYRtnkvA
jp1q7Hg2YHi7ghuHKhENsSK1PPeTq7WD3S5vqEnkIfp8SYBDnJ9Y6j999q3zCayn
gxomoEu2/Vr+mGHeMh07jf6/8L1lJLAemxI16T2sfenPaYOs3Kh2f+44psKmuaEt
c58zVNPl8aSVTDS4jjntWeYOEk4HldT10GcwKpnOCrX6J7PLFvwyiVbede7SED13
ePnGgTPVW15xF6vD+veqRiYpFMw+uUX8HiJb++jHuQINBGoBjNkBEAC2CP7S1Tvd
k5MhK7j/xu9hgQzcrjiN8yIwpTdRxzJ/z9AxoSHWzC4tFZFdKVl9PFGNuQoONTKT
lf3Rt6pNCgZfRYZSL94JQMSQoyTq5s8N5y4J2th9L1+nQhdSZfrDeruihuuyVRz4
yaZhzRvuDvv2s6egHZM8Ev66fJF77ZAQ16HU487GPfUmWzw5KW/EyNvfCTqhaNtZ
NnnP6+RSLMQ4ct/EGfIvc1Omnaef7uz56BpQFBR1VKGrweEOJkevynKid7MqpxfN
2gngGhPSLlFEo1EkqyeyU3xfNvJ2+qiYdhxm/f5aVHQKPwBJ6xD6qmn6Y+xvy4az
9bT8vBvrVQwkXalrB+L8T11MEzPY9g/SX9t1y3/wfUork6BdMEqRwdeyFDnIhXe9
whhvVE3vz0SCeXFqXA1QVYgOXMLr6+WmhAOTpGjVHPnz5A4Tfi/qHoTYfDqQDyY+
gyyavsrwADgb+X/0LtOc7kw4HjR9zdHK/TCltBCUK+Vl6q3zepoQO29vx5fnOoJX
pMbILZC/5hTPMgnpEK75KMB/PBgOBSsDf9HXqBWDjCKQ0BfL2RM+451Rxminej6N
0FwHvXFefr/xdNoupT176Nrn2WcLmmtR5voVjN5GRYOpiTtDss3gyMEg1zYo5Lfl
iEZ3vGFPWS2fH1X4anEnjaBFT9Z8qW15AwARAQABiQI2BBgBCAAgFiEELtI9DcMS
xwu7if66fQptAstz2DgFAmoBjNkCGwwACgkQfQptAstz2Djibg//bQBCL+fU8ACY
```

```
VnADKxQMh6UVlgyebWPfQeEuRYwtQ2QsiI2wKrM0W6FV6mJHmcT2rpvz3pUViqPv
XZd2/I5ShVCGhLmObwxQFQLSDkDLD2J5QDcNM8GTWzlaxWm481+xkrjM5SgKNo9C
VnDBtzPE31vwAk/icD7ahRKelgTRm5MI2KjRjLcIRyBoWH81yS2Uxs6cX3UCYwzc
n2xjg2ez7AWTbnkg3FThYRRJm7X25imZ1FZz8NQqNZlXKCdbg1a97/NpSpXfGD+u
oZZjzSBkuMEgNAIZx7vT/wNQzm9SJOkPKDWUX498hnG+tDcjjXSclunSCtonl2CM
7jDzetm38r36CCNvDz4U4HimsauN4JSxTbA7JBQaiu2DT3lyEmkOfxH33wQ6gceV
lJe2CKdbjn8RSvvPHzvhTifzEJhrvFTduSOQuaGbhQIEvn6QShE1V+O3wWpcAggM
Qluee33f6Y9hs91YkMz21UZ830dOKohE42tS/wDmWBJq7+5YpuuapPQqcSqxBgoD
GxeoUDiHGTfSm+gt5z8lzI5yRUOvUq7ttjCnwZXEcJf0DT1FqfUyITsKi0PCu65i
qLos6Kz+WgasyRkvg9NNMHOuV2al+XPxOmNcIXyUBRXiKXlHf7VGUSq6JDeVHCba
yQaQbrJ3faWx/F01nDQLnnNLChqCVFI=
=zBF3
-----END PGP PUBLIC KEY BLOCK-----
```

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

- Please use this key when you want/need to encrypt messages that you send to CERT-XMCO.
- When due, CERT-XMCO will sign messages using the same key.
- When due, sign your messages using **your own key** please. It helps when that key is verifiable (for instance, using the public keyservers).

2.9 Team Members

CERT-XMCO's team leader is François DEBRY.

The team consists of XMCO's IT security analysts.

2.10 Other Information

General information regarding CERT-XMCO can be found at the following URL:

- https://www.xmco.fr/#section-home-cert

CERT-XMCO is listed by the *Trusted Introducer* for CERTs in Europe, see:

- https://www.trusted-introducer.org/trusted-introducer/directory/teams/cert-xmco-fr/

2.11 Points of Customer Contact

The preferred method to contact CERT-XMCO team is to send an email to the cert@xmco.fr address, which is monitored during hours of operation.

Urgent cases can be reported by phone during regular office hours on +33 (0)1 47 34 30 38.

You can also reach the CERT-XMCO by phone if it is not possible (or not advisable for security reasons) to use email.

- *Days/Hours of Operation*: 09:00 to 18:00 local time, Monday to Friday (except public holidays in France).
- Out of office hours operation in case of emergency.

3. Charter

This section describes CERT-XMCO's mandate.

3.1 Mission Statement

CERT-XMCO is a private CSIRT team delivering Security services, mainly in France.

Its purpose is two-folded:

- First, to assist its customer community in **implementing proactive measures to reduce the risks of computer security incidents**.
- And second, to assist its customer community in **responding to such incidents** whenever they occur.

CERT-XMCO's mission is to support its customer community to protect themselves against both intentional and opportunistic attacks that would hamper the integrity of their IT assets and harm their interests. The scope of CERT-XMCO's activities covers prevention, detection, response and recovery. CERT-XMCO is in charge of digital forensics and incident response (DFIR) activities.

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

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

3.2 Constituency

CERT-XMCO's *primary constituency* is composed of all the elements of XMCO's Information System: its users, its systems, its applications and its networks.

However, notwithstanding the above, CERT-XMCO's services are also delivered to a *secondary constituency*. As a commercial CSIRT, the CERT-XMCO also provides services to its Customers Community, who subscribed a *Service Level Agreement* support contract.

Current customers which are located in France and other countries are found among:

- Private sector organisations
- Public sector bodies
- Commercial bodies

3.3 Sponsorship and/or Affiliation

CERT-XMCO is part of XMCO: https://www.xmco.fr/.

CERT-XMCO maintains contact with various national and international CSIRT and CERT teams (mainly throughout France), on an as-needed basis.

3.4 Authority

CERT-XMCO coordinate security incidents on behalf of its constituency, and only at its constituents' request.

Consequently, CERT-XMCO operates under the auspices of, and with authority delegated by its constituents.

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

Generally, CERT-XMCO expects to work cooperatively with its constituents' system administrators and users.

4. Policies

This section describes CERT-XMCO's policies.

4.1 Types of Incidents and Level of Support

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

The level of support given by CERT-XMCO will vary depending on the type and severity of the incident or issue, its potential or assessed impact, the type of constituent, the size of the user community affected, and CERT-XMCO's resources at the time. Depending on the security incident’s type, CERT-XMCO will gradually roll out its services which include incident response and digital forensics. In all cases, some response will be made within two working days.

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

All incidents are considered normal priority unless they are labelled EMERGENCY. CERT-XMCO itself is the authority that can set and reset the EMERGENCY label. An incident can be reported to CERT-XMCO as EMERGENCY, but it is up to CERT-XMCO to decide whether to uphold that status.

CERT-XMCO 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. This communication will be in the form of: Email alerts, or phone calls under certain circumstances.

Note that no direct support will be given to end users. They are expected to contact their Security Operation Center (SOC) or internal CSIRT for assistance. The CERT-XMCO will support the latter people.

4.2Co-operation, Interaction and Disclosure of Information

CERT-XMCO considers the paramount importance of operational coordination and information sharing between CERTs, CSIRTs, SOCs and similar bodies, and also with other organizations which may contribute towards or make use of their services.

Consequently, CERT-XMCO exchanges all necessary information with affected parties, as well as with other CSIRTs, on a need-to-know basis. However, neither personal nor overhead data are exchanged unless explicitly authorised. Moreover, CERT-XMCO will protect the privacy of its customers/constituents, and therefore (under normal circumstances) pass on information in an anonymised way only (unless other contractual agreements apply).

All incoming information is handled confidentially by CERT-XMCO, 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 environment as stated below.

CERT-XMCO supports the Information Sharing Traffic Light Protocol version 2.0 (ISTLP, see https://www.trusted-introducer.org/documents/11/ISTLP.pdf). Information that comes in with the tags WHITE, GREEN, AMBER or RED will be handled appropriately.

CERT-XMCO operates within the current French legal framework. and, complies with the CCoP (CSIRT Code of Practice) version 2.4 (see https://www.trusted-introducer.org/documents/13/TI-CCoP.pdf).

4.3 Communication and Authentication

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

CERT-XMCO respects the sensitivity markings allocated by originators of information communicated to CERT-XMCO (“originator control”).

CERT-XMCO also recognises and supports the ISTLP version 2.0.

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

- Telephones will be considered sufficiently secure to be used (even unencrypted), in view of the types of information that CERT-XMCO deals with.
- Unencrypted email will not be considered particularly 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 2.8). Network file transfers will be considered to be similar to email for these purposes: sensitive data should be encrypted for transmission.

---

5. Services

This section describes CERT-XMCO's services.

These services are primarily delivered to CERT-XMCO's customers.

5.1 Announcements

CERT-XMCO provides information on the threat landscape, published vulnerabilities, new attack tools or artifacts and security measures needed to protect its constituency’s Information System.

5.2 Alerts and Warnings

CERT-XMCO disseminates information on cyberattacks, disruptions, security vulnerabilities, intrusion alerts, malware, and provides recommendations to tackle the issue within its constituency.

Alerts and warnings may be passed on to other CERTs, CSIRTs, SOCs and similar bodies if deemed necessary or useful to them on a need-to-know basis.

CERT-XMCO is not responsible for the implementation of its recommendations. Incident resolution is usually left to the responsible administrators within the constituency. However, CERT-XMCO will offer support and advice on request.

5.3 Pre-emptive Security Controls

CERT-XMCO performs pre-emptive security controls to detect potential breaches or vulnerabilities and misconfigurations that may be leveraged in cyberattacks. The security controls also check the compliance level of various systems and applications with the security policies.

This service is primarily delivered to CERT-XMCO's customers.

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

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

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

CERT-XMCO will assist IT Security team in handling the technical and organisational 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 indeed an incident occurred
    - by determining the extent of the incident
- Incident Coordination:
    - by determining the initial cause of the incident (vulnerability exploited)
    - 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 CSIRTs (if applicable)
- Incident Resolution
    - by fixing the vulnerability
    - by securing the system from the effects of the incident
    - by evaluating whether certain actions are likely to reap results in proportion to their cost and risk
    - by collecting evidence where criminal prosecution, or disciplinary action, is contemplated
    - by collecting statistics concerning incidents which occur within or involve its constituency

CERT-XMCO's incident response service tries to cover at best all the ‘6 steps’: preparation, identification, containment, eradication, recovery and lessons to be learned.

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

5.5 Development of Security Tools

CERT-XMCO internally develops security tools for its own use, to support its activities and improve its services.

Even though these security tools are used to provide benefits to CERT-XMCO's constituency, they are not to be shared/used neither by members of its constituency or by members of the larger CERT, CSIRT and SOC communities.

6. Incident Reporting Forms

No local form has been developed to report incidents to CERT-XMCO.

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

- contact details and organisational information (contact name, organisation name and address);
- email address, telephone number;
- IP address(es), FQDN(s), and any other relevant technical element with associated observation;
- if any, scanning results or extract from the log showing the problem;
- in case you wish to forward any emails, please include all email headers, body and any attachments if possible and as permitted by the regulations, policies and legislation under which you operate.

7. Disclaimers

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