SÉCURITÉ NUMÉRIQUE

CERT ON-X

RFC 2350

Description of services

Date : 02/04/2021

Référence : ON-X_CERT_RFC2350

Version : 1.0

Pages : 10

[Public diffusion - TLP : WHITE]

GROUPE

PARIS | TOULOUSE | MONTBÉLIARD | LYON

Siège social - 15 quai de Dion Bouton - F-92800 Puteaux
Tel : +33 (0)1 40 99 14 14 | Fax : +33 (0)1 40 99 99 58 | e-mail : contact@on-x.com

TABLE OF CONTENT

1. ABOUT THIS DOCUMENT

This document contains a description of the ON-X Computer Emergency Response Team (CERT) / Computer Security Incident Response Team (CSIRT) according to the document RFC 2350[1].

It provides essential information about CERT ON-X, its role, its responsibilities and means of communication.

1.1. DATE OF LAST UPDATE

This is version 1.0, published 02/04/2021.

1.2. DISTRIBUTION LIST FOR NOTIFICATIONS

No distribution list.

1.3. LOCATIONS WHERE THIS DOCUMENT MAY BE FOUND

The current version of this CERT description document is available from the ON-X's web site: https://www.on-x.com/contact

Please make sure you are using the latest version.

1.4. AUTHENTICATING THIS DOCUMENT

This document has been signed with the CERT ON-X's PGP key. The signature is also on ON-X's web site: https://www.on-x.com/contact

[1] https://tools.ietf.org/html/rfc2350

2. CONTACT INFORMATION

This section describes CERT ON-X's means of communication.

2.1. NAME OF THE TEAM

"CERT ON-X": the ON-X Computer Emergency Response Team (CERT) / Computer Security Incident Response Team (CSIRT).

2.2. ADDRESS

ON-X
15 quai de Dion-Bouton
92800 Puteaux
FRANCE

2.3. TIME ZONE

Central European Summer Time (UTC +1, and UTC +2 for Daylight Saving Time which starts on the last Sunday in March and ends on the last Sunday in October)

2.4. TELEPHONE NUMBER

+33 1 40 99 29 99

2.5. FACSIMILE NUMBER

Not available.

2.6. OTHER TELECOMMUNICATION

Online Video conferencing is available on request.

2.7. ELECTRONIC MAIL ADDRESS

The CERT ON-X email address is: cert(at)on-x.com.

This e-mail address is read by the entire CERT team.

2.8. PUBLIC KEYS AND OTHER ENCRYPTION INFORMATION

The CERT ON-X has a PGP key whose:

- **User ID**: CERT ON-X <cert(at)on-x.com>
- **KeyID**: 0x8C7BCBC0
- **Fingerprint**: 25E1 B6A3 59DB 5AD4 8E8B 12FA 0676 8BC9 8C7B CBC0

The key and its signatures can be found at:

- ON-X's web site: https://www.on-x.com/contact
- The usual large public keyservers such as http://pgp.mit.edu

2.9. TEAM MEMBERS

Olivier REVENU is the CERT ON-X coordinator. The team is made up of ON-X's cybersecurity analysts.

2.10. OTHER INFORMATION

General information about ON-X and CERT ON-X can be found at https://www.on-x.com.

2.11. POINTS OF CUSTOMER CONTACT

The preferred method for contacting the CERT ON-X is via e-mail at cert(at)on-x.com .

If it is not possible (or not advisable for security reasons) to use e-mail, the CERT ON-X can be reached by telephone during regular office hours.

The CERT ON-X's hours of operation are generally restricted to regular business hours (09:00-18:00 Monday to Friday except holidays).

In case of emergency and outside working hours, the CERT ON-X's telephone is redirected to a member's mobile number.

3. CHARTER

This section describes CERT ON-X's mandate.

3.1. MISSION STATEMENT

CERT ON-X is a commercial CERT delivering services mainly in France with two purposes:

- first, to assist customers in implementing proactive measures to reduce the risks of computer security incidents;
- second, to assist customers in responding to such incidents when they occur.

3.2. CONSTITUENCY

The CERT ON-X's constituency is composed of:

- all elements of ON-X's Information System (users, systems, applications, and networks);
- its customers as described in the performance contract.

3.3. SPONSORSHIP AND/OR AFFILIATION

The CERT ON-X is part of ON-X GROUPE SAS.

3.4. AUTHORITY

For internal matters, CERT ON-X operates under the authority of the Associate Director in charge of Cybersecurity Business Unit.

For customers' incidents, CERT ON-X investigates and coordinates security incidents on behalf of its constituency, and only at its constituents' request. However, it does not have formal authority over its constituency.

4. POLICIES

This section describes CERT ON-X's policies.

4.1. TYPES OF INCIDENTS AND LEVEL OF SUPPORT

CERT ON-X addresses all types of computer security incidents which occur, or threaten to occur, at its constituency.

The level of support given by CERT ON-X 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 ON-X's resources at the time.

4.2. CO-OPERATION, INTERACTION AND DISCLOSURE OF INFORMATION

CERT ON-X considers the paramount importance of operational coordination and information sharing between CERTs, CSIRTs, SOCs and similar bodies, and also with other organizations, which may aid to deliver its services or which provide benefits to CERT ON-X's constituency.

Consequently, CERT ON-X 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 authorized. Moreover, CERT ON-X 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 ON-X, 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 ON-X supports the Information Traffic Light Protocol (TLP[2]). Information that comes in with the tags WHITE, GREEN, AMBER or RED will be handled appropriately.

CERT ON-X operates within the current French legal framework.

4.3. COMMUNICATION AND AUTHENTICATION

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

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

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

CERT ON-X also recognizes and supports the Information Traffic Light Protocol (TLP).

As far as possible, CERT ON-X use secure data communications with its constituents:

- E-mail can be handled by using PGP;
- File sharing, particularly for large files, can be handled with a dedicated sharing solution using HTTPS.
- Discussions can be handled on a videoconference solution using HTTPS or by phone if not too sensitive.
- In case of identity doubt or technical risk for identity theft, CERT ON-X will use a second channel to confirm the identity.

5. SERVICES

This section describes CERT ON-X's services.

5.1. PROACTIVE ACTIVITIES

CERT ON-X coordinates and maintains the following services to the extent possible depending on its resources:

- risk analysis;
- security consulting;
- security awareness;
- security assessments and penetrations tests;
- vulnerabilities management;
- intrusion detection and response services.

5.2. DIGITAL FORENSICS AND INCIDENT RESPONSE

CERT ON-X will assist its constituency in handling the technical and organizational aspects of incident responses.

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

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

6. INCIDENT REPORTING FORMS

There are no local forms developed yet for reporting incidents to CERT ON-X.

If possible, please provide 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 with any relevant technical elements;
- affected assets, impact;
- actions taken so far.

7. DISCLAIMERS

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

END OF DOCUMENT

ON-X GROUPE

ACCÉLÉRATEUR DU NUMÉRIQUE

5 Pôles de compétences

- X REALITY
- INFRA NUMÉRIQUE
- SÉCURITÉ NUMÉRIQUE
- TERRITOIRES NUMÉRIQUES
- SYSTÈME D'INFORMATION

3 Services Cloud, RGPD & Blockchain

La FRENCH TECH

Quality Management ISO 9001

LAVAL VIRTUAL university

CABINET DE CONSEIL **FRANÇAIS** | **INDÉPENDANT** | **EXPERT**

DEPUIS **1986**