1. Document Information

This document contains a description of CERT-FR in accordance with RFC 2350[1] specification. It provides basic information about CERT-FR, describes its responsibilities and services offered.

1.1. Date of Last Update

Version 1.0, published on 2018-12-14.

1.2. Distribution List for Notifications

Changes to this document are notified by email to:

- InterCERT-FR / network of French CSIRTs - www.cert.ssi.gouv.fr/csirt/intercert-fr
- ENISA and CSIRTs Network members - www.enisa.europa.eu
- Trusted Introducer service - www.trusted-introducer.org
- FIRST organisation - www.first.org

Please send questions about updates to CERT-FR team email address: cert-fr.cossi[at]ssi.gouv.fr

1.3. Locations where this Document May Be Found

The current and latest version of this document is available on the CERT-FR's website at:
www.cert.ssi.gouv.fr/about-us/CERT-FR_RFC2350_EN.html

1.4. Authenticating this Document

This document has been signed with the PGP key of CERT-FR.
The PGP public key, ID and fingerprint are available on the CERT-FR's website at:
www.cert.ssi.gouv.fr/contact

1.5. Document Identification

Title: 'CERT-FR_RFC2350_EN'
Version: 1.0
Document Date: 2018-12-14
SHA-256
Expiration: this document is valid until superseded by a later version

[1] www.ietf.org/rfc/rfc2350.txt

2. Contact Information

2.1. Name of the Team

Official name:
Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (French government computer emergency response team).
Short name:
CERT-FR

2.2. Address

Secrétariat général de la défense et de la sécurité nationale
SGDSN/ANSSI/CERT-FR
51 boulevard de La Tour-Maubourg
75007 Paris, FRANCE

2.3. Time Zone

CET/CEST

2.4. Telephone Number

Main number (duty office): +33 1 71 75 84 68

2.5. Facsimile Number

Fax number: +33 1 84 82 40 70

2.6. Other Telecommunication

Not applicable

2.7. Electronic Mail Address

If you need to notify us about an information security incident or a cyber-threat targeting or involving CERT-FR, please contact us at: cert-fr.cossi[at]ssi.gouv.fr

2.8. Public Keys and Encryption Information

PGP is used for functional exchanges with CERT-FR.

- User ID: CERT-FR <cert-fr.cossi[at]ssi.gouv.fr>
- Key ID: 0x1B45CF2A
- Fingerprint: 7F4C 8FA6 A356 D1CC 2E5C AB09 5416 33B8 1B45 CF2A

The public PGP key is available at: www.cert.ssi.gouv.fr/uploads/public_key.asc
It can be retrieved from one of the usual public key servers.

2.9. Team Members

The list of the CERT-FR's team members is not publicly available. The identity of CERT-FR's team members might be divulged on a case by case basis according to the need to know restrictions.

2.10. Other Information

See our web site at www.cert.ssi.gouv.fr for additional information about CERT-FR.

2.11. Points of Customer Contact

CERT-FR prefers to receive incident reports via e-mail at cert-fr.cossi[at]ssi.gouv.fr. Please use our cryptographic key to ensure integrity and confidentiality. In case of emergency, please specify the [URGENT] tag in the subject field in your e-mail.

CERT-FR's hours of operation are 7/7 24h all year long.

3. Charter

3.1. Mission Statement

CERT-FR is the Computer Emergency Response Team (CERT) of the French national cyber security authority. Its mission is to coordinate and investigate IT security incident response for the French government, critical national infrastructure operators and operators of essential services as defined by the French law.

CERT-FR's missions cover prevention, detection, response and recovery by:

- Helping to prevent security incidents in set up necessary protection measures;
- Detecting vulnerabilities on networks and systems;
- Managing incident response, with the support of trusted partners if necessary;
- Organizing trusted networks of CSIRT.

3.2. Constituency

The primary constituency is composed of all French territories (DROM-COM included) and cover:

- All ministries, administrations and state services;
- Critical national infrastructure operators and operators of essential services as defined by the French law;
- Other key players in sensitive sectors.

More information can be found on the Agence nationale de la sécurité des systèmes d'information (ANSSI) website: www.ssi.gouv.fr.

3.3. Affiliation

CERT-FR is part of the Agence nationale de la sécurité des systèmes d'information (ANSSI), the French national cyber security agency acting as national cyber-security authority.

3.4. Authority

French Prime Minister services
SGDSN – Secretary General for Defence and National Security
ANSSI/CERT-FR operates under the SGDSN

4. Policies

4.1. Types of Incidents and Level of Support

CERT-FR is the central point of contact regarding security-related computer incidents in France.
The level of support given by ANSSI will vary depending on the type and severity of the incident or issue, the type of constituent, the importance of the impact on critical or essential infrastructure or services, and the CERT-FR resources at the time.
CERT-FR's services include reactive and proactive services:

- 24-hour on-call duty;
- Alerts and warnings;
- Incident analysis and forensics;
- Incident response assistance and support;
- Incident response and remediation;
- Vulnerability and malware analysis;
- Vulnerability response;
- Threat intelligence analysis and sharing.

In addition, CERT-FR liaises and is able to request to a matrix of other expertise and knowledge provided by other French government offices.

4.2. Co-operation, Interaction and Disclosure of Information

General incident related information such as names and technical details is not published without agreement of the named parties. If not agreed otherwise, supplied information is kept confidential. CERT-FR will never pass information to third-parties unless required by law. Under the condition of acceptance through affected parties or authorized by law, CERT-FR prefers to share Tactics, Techniques and Procedures for the purpose of prevention and reaction to specific incidents.

Therefore such information might be passed to entities such as:

- ANSSI's own technical experts;

- Affected parties in our constituency;
- Affected ISPs/hosting providers in France;
- French law enforcement agencies (if required by law or on request from information source);
- CERT/CSIRT cooperation groups as named in Section 1.2;
- Trusted Partners having ANSSI Security Visas (see www.ssi.gouv.fr/en/security-visa).

All information is passed depending on its classification and the need-to-know principle. Only the specifically relevant and anonymised extracts are passed on. CERT-FR respects the Information Sharing Traffic Light Protocol (TLP) that comes with the tags WHITE, GREEN, AMBER or RED as described by the FIRST definitions at: www.first.org/tlp/

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

4.3. Communication and Authentication

The preferred method of communication is email. For the exchange of sensitive information and authenticated communication CERT-FR uses several encryption solutions. By default, all sensitive communication to CERT-FR should be encrypted with our public PGP key detailed in Section 2.8.

5. Services

5.1. Incident response

CERT-FR's incident response services are available on a 24/7 basis to our constituency. All information and communication technologies related incidents are evaluated. In-depth analysis is provided by technical experts.

5.2. Incident Triage

- Assessment of the severity of the incident. First level of response.
- If required, escalation to the duty officer. Second level of response.
- If required, escalation to the general management.

5.3. Incident Coordination

- Categorization of the incident related information with respect to the information disclosure policy.
- Notification of other involved parties on a need-to-know basis, as per the information disclosure policy.

5.4. Incident Resolution

- This may include analysis of compromised systems.

- Elimination of the cause of a security incident (the vulnerability exploited) and its effects (for example, continuing access to the system by an intruder).

5.5. Proactive activities

- Warning and information services available on www.cert.ssi.gouv.fr portal.
- Cyber daily news and advisory mailing list.
- Network monitoring to detect attacks as early as possible.
- Training security officers from administrations and public sector.

Several departments of ANSSI offer additional services such as education, product certification, security auditing, consulting etc. More information on ANSSI's services is available on ANSSI's institutional web site www.ssi.gouv.fr.

6. Incident Reporting Forms

The reporting of security incidents involving the government, critical national infrastructure operators, operators of essential services and digital service providers is based on specific secured reporting forms and procedures. No specific form is needed to report security incidents from other parties.

7. Disclaimers

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