RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

TLP:CLEAR

CERT-FR

RFC 2350

Version 1.3 - 2024-08-13

CERT-FR

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 1.3, published on 2024-08-13.

1.2. Distribution list for notifications

Changes to this document are notified to:

- InterCERT France / network of French CSIRTs – https://www.intercert-france.fr/
- ENISA – https://www.enisa.europa.eu/
- EU CSIRTs Network members – https://www.csirtsnetwork.eu/
- FIRST – https://www.first.org/
- Task Force CSIRT (TF-CSIRT) – https://www.trusted-introducer.org/

Please send questions about updates to CERT-FR team email address: cert-fr@ssi.gouv.fr

1.3. Locations where this document may be found

The current and latest version of this document is available at CERT-FR's website at: https://cert.ssi.gouv.fr/uploads/CERT-FR_RFC2350_EN.pdf

1.4. Authenticating this document

This document has been signed with the PGP key of CERT-FR. The signature and our public PGP key (ID and fingerprint) are available on our website: https://cert.ssi.gouv.fr/contact

1.5. Document identification

Title: 'CERT-FR_RFC2350_EN'
Version: 1.3
Document Date: 2024-08-13
Expiration: this document is valid until superseded by a later version

1 https://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
75700 Paris 07 SP, FRANCE

2.3. Time zone

CET/CEST

2.4. Telephone number

Main number (duty office): **+33 9 70 83 32 18**
Short number (from France only): **32 18**

2.5. Facsimile number

Not applicable

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@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@ssi.gouv.fr>
- Key ID: 0x1B45CF2A
- Fingerprint: 7F4C 8FA6 A356 D1CC 2E5C AB09 5416 33B8 1B45 CF2A

The public PGP key is available at the following location:
https://cert.ssi.gouv.fr/contact/
It can be retrieved from one of the usual public key servers such as https://pgp.circl.lu/ or https://pgp.mit.edu/.

2.9. Team members

CERT-FR team is composed of IT security experts. The list of CERT-FR team's members is not publicly available. The identity of CERT-FR team's 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 https://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@ssi.gouv.fr. Please use our cryptographic key to ensure integrity and confidentiality. In case of emergency, please use the [URGENT] tag in the subject field in your e-mail.

CERT-FR's hours of operation are 24/7.

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 prevent security incidents by setting up necessary protection measures;
- Detecting vulnerabilities on networks and systems;
- Sharing information on cyber threats with its constituents and partners;
- Managing incident response with the support of trusted partners if necessary;
- Participating in trusted networks of CSIRTs.

3.2. Constituency

CERT-FR primary constituents are located across all French territories (including overseas territories of France) and include:

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

Secondary constituents are all private sector organisations registered in France that do not provide essential services, and can also benefit from a limited number of services from CERT-FR.

In order to have more information, please take a look at the ANSSI website https://cyber.gouv.fr/.

3.3. Affiliation

CERT-FR is part of ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), the French National Cyber Security Agency acting as national cyber authority.

3.4. Authority

French Prime Minister Services
SGDSN –General Secretariat 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 service, and the CERT-FR available resources at the time.
CERT-FR's services include reactive and proactive services:

- 24/7 on-call duty;
- alerts and warnings;

- incident analysis and forensics;
- incident response assistance and support;
- incident response and remediation (also on-site);
- vulnerability and malware analysis;
- vulnerability response;
- threat intelligence analysis and sharing.

4.2. Co-operation, interaction and disclosure of information

Incident-related information, such as names and technical details, is not published without agreement of involved stakeholders. If not agreed otherwise, supplied information is kept confidential. CERT-FR will never pass information to third parties unless required by law.

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 by information source);
- CERT/CSIRT cooperation groups as named in Section 1.2;
- Trusted Partners having ANSSI Security Visas (see https://cyber.gouv.fr/en/security-visa).

CERT-FR is deeply engaged in national, European and international cooperation groups (see 1.2) and strongly supports voluntary cooperation between CSIRTs at all levels. For that matter, CERT-FR ensures a global presence and networking with its partners through an active participation in working groups and international meetings and conferences.

CERT-FR is also able to receive and process reports about suspicious activities or incidents about any entity or product within its constituency, as well as vulnerability reports (see https://cyber.gouv.fr/signaler-une-vulnerabilite-un-incident) from its constituents or from any individual.

Within CERT-FR, information is passed depending on its classification and need-to-know principle and thus only the specifically relevant and anonymised extracts are passed on.

When CERT-FR is provided with information enforcing the Traffic Light Protocol (TLP), it respects the information sharing policy defined by the FIRST at: https://www.first.org/tlp/.
For operational information originating from CERT-FR, with both TLP and PAP markings, the sharing and using policy, as defined at https://cert.ssi.gouv.fr/csirt/sharing-policy/, is to be considered by the recipients.

4.3. Communication and authentication

The preferred method of communication is email. For the exchange of sensitive information and authenticated communication CERT-FR uses PGP for encrypting and/or signing messages. All sensitive communication to CERT-FR should be encrypted with our public PGP key as 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 (log files, contact information, etc.) 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

- Analysis of compromised systems;
- Elimination of the cause of a security incident (exploited vulnerability), and its effects.

5.5. Proactive activities

- Warning and information services available at https://cert.ssi.gouv.fr/;

- Cyber daily news and advisory mailing list;
- Network monitoring to detect attacks as early as possible;
- Training security officers from administrations and public sector.

5.6. Vulnerability management

- Vulnerability discovery and research;
- Handling of vulnerability reports;
- Vulnerability analysis;
- Assistance to vulnerable product vendors in the release of Common Vulnerabilities and Exposures (CVE) reports;
- Coordinated vulnerability disclosure (CVD).

5.7. Cyber threat analysis

- Sharing and publication of cyber threats alerts and reports;
- Provision of feeds of Indicators of Compromise (IOCs) to help constituents and partners detect and prevent threats, and to analyse incidents;
- Sharing and publication of periodic threat landscape reports.

Other departments of ANSSI offer additional services such as education, product certification, security auditing, consulting, etc. More information on ANSSI's services is available at ANSSI institutional web site https://cyber.gouv.fr/.

6. Incident reporting forms

The reporting of security incidents from government or critical national infrastructure operators is based on specific secured reporting form and procedure (see https://cyber.gouv.fr/notifications-reglementaires). No special forms are 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.