CERT ITRUST-FREE RFC-2350

V.1 07/2024

Sommaire

1 Document information

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

1.1 Date of last update

The current version of this document is **version 1.0** and was released on **July 2nd, 2024**.

1.2 Distribution List for Notifications

There is no Distribution List, or other dissemination mechanism to inform about changes made to this document.

1.3 Locations where this document may be found

The current and latest version of this document is available at ITRUST's website at:
https://www.itrust.fr/wp-content/uploads/2024/07/CERT_ITRUST_RFC2350_EN.pdf

1.4 Authenticating this document

This document has been signed with the PGP key of CERT ITRUST-FREE. The signature and our public PGP key (ID and fingerprint) are available on our website:
https://www.itrust.fr/cert/

1.5 Document identification

Title: 'CERT_ITRUST_RFC235_EN'
Version: 1.0
Document Date: 02/07/2024
Expiration: this document is valid until superseded by a later version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

Short name: CERT ITRUST-FREE
Full name: CERT ITRUST-FREE

2.2 Address

CERT ITRUST-FREE

ISSY-LES-MOULINEAUX (FRANCE):
- 6 Rue du 4 Septembre, 92130 Issy-les-Moulineaux

LABÈGE (FRANCE):
- 1000 L'Occitane, 31670 Labège

2.3 TimeZone

CET/CEST Europe/Paris (GMT+01:00, and GMT+02:00 on DST)

2.4 Telephone Number

+33(0)5.67.34.67.83

2.5 Facsimile number

Not available

2.6 Other telecommunication

Not available

2.7 Electronic mail address

If you need to notify us about an information security incident or a cyber-threat targeting or involving CERT ITRUST-FREE, please contact us at: cert@itrust.fr

2.8 Public Keys and Encryption Information

PGP is used for functional exchanges with CERT ITRUST-FREE.
User ID: CERT ITRUST <cert@itrust.fr>
Key ID: 0x5A851E0E3B5B55AF
Fingerprint: 1A4E B8B5 35F8 808E 5668 AED7 5A85 1E0E 3B5B 55AF

The public PGP key is available at the following location: https://www.itrust.fr/cert/

2.9 Team Members

The CERT ITRUST-FREE team consists of IT security experts. The list of team members is not publicly disclosed. The identities of team members may be revealed on a case-by-case basis, depending on need-to-know requirements.

2.10 Other Information

See our web site at itrust.fr for additional information about CERT ITRUST-FREE

2.11 Points of Customer Contact

CERT ITRUST-FREE prefers to receive incident reports via e-mail at cert@itrust.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 ITRUST-FREE hours of operation are 24/7

3 Charter

3.1 Mission statement

CERT ITRUST-FREE is a private CERT dedicated to ITRUST and FREE/ILIAD customers. Its services are available to organizations that have subscribed to CERT ITRUST-FREE services.

CERT ITRUST-FREE has various missions including:

- Incident Response: Provide timely and effective response to cybersecurity incidents.
- Analysis and Reporting: Analyze security incidents and produce detailed reports for stakeholders.
- Coordination and Collaboration: Collaborate with other security teams, organizations, and law enforcement agencies.
- Education and Prevention: Educate users on security best practices and implement preventive measures to minimize risks.
- Surveillance and Mass Prevention: Conducting continuous surveillance and large-scale prevention efforts while serving as a liaison with government agencies.

3.2 Constituency

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

3.3 Sponsorship and/or affiliation

CERT ITRUST-FREE is a private CERT in the cybersecurity sector. It is owned, operated and financed by ITRUST and FREE.

3.4 Authority

CERT ITRUST-FREE handles incident responses for customers and advises local security teams without having the authority to enforce specific actions. Any recommendations made by CERT ITRUST-FREE will be carried out according to the customer's direction.

4 Policies

4.1 Types of incidents and Level of support

CERT ITRUST-FREE is generally mandated by its customers to handle any type of incident occurring within their own perimeter. However, CERT ITRUST-FREE manages all types of cybersecurity incidents that occur, or threaten to occur, within its constituencies.

CERT ITRUST-FREE 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

CERT ITRUST-FREE operates under the restrictions imposed by French laws.

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 ITRUST-FREE will never pass information to third parties unless required by law.

CERT ITRUST-FREE uses the Traffic Light Protocol (TLP) in accordance with ANSSI recommendations.

CERT Team will cooperate with other Organizations in the field of Computer Security, which may help to deliver its services, especially for incident resolution.

4.3 Communication and authentication

The preferred method of communication is email. For the exchange of sensitive information and authenticated communication, CERT ITRUST-FREE uses PGP for encrypting and/or signing messages.

All sensitive communication to CERT ITRUST-FREE should be encrypted with our public PGP key as detailed in this document.

5 Services

5.1 Incident response

CERT ITRUST-FREE'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

1. Organizing incident-related data such as log files and contact details according to the information disclosure guidelines.
2. Informing relevant parties involved only when necessary, in accordance with the information disclosure policy.

5.3 Incident Coordination

1. Classifying incident-related information (including log files and contact details) in alignment with the information disclosure policy.
2. Collection of technical evidence
3. Identification of the perimeter impacted by the incident
4. Proposition of immediate corrective measures
5. Determining the initial cause of the incident

6. Notifying other relevant parties selectively, following the information disclosure policy's need-to-know principle.

5.4 Incident Resolution

- Proposal for sustained corrective actions
- Informal feedback provided to the team affected by the incident
- Conducting a forensic investigation report as needed

5.5 Proactive activities

- Cyber daily news and advisory mailing list
- Webinar
- Cyber security blogpost and publications
- Knowledge gathering on cyber threat actors
- Reflex Datasheet for incident handling

5.6 Vulnerability management

- Vulnerability discovery and research
- Handling of vulnerability reports
- Vulnerability analysis

6 Incident reporting forms

CERT ITRUST-FREE does not have a public incident reporting form.

7 Disclaimer

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