CERT I-TRACING
RFC 2350
DECEMBER 2022

I-TRACING – Workstation, 25 quai du Président Paul Doumer, CS30133, 92408 Courbevoie Cedex,
FRANCE – P: 01 70 94 69 70 – Fax: 01 70 94 69 71
Société par Actions Simplifiées – SIREN 484841127 RCS Nanterre NAF Code 6202A

Document follow-up

Document details	
Title:	CERT I-TRACING RFC 2350
Object:	CERT I-TRACING RFC 2350 specifications details
Diffusion:	Without restriction. Subject to copyright controls
Reference:	ITR-CERT-RFC2350-EN-1.2
Last update:	7 December 2022
Version:	1.2
Validity:	This document is valid until superseded by later version.

I-TRACING ©2022 – Reproduction prohibited without explicit permission

TABLE OF CONTENTS

1. DOCUMENT INFORMATION 6
   1.1. Date of Last Update 6
   1.2. Distribution List for Notifications 6
   1.3. Locations where this Document May Be Found 6
   1.4. Authenticating this Document 6
   1.5. Document Identification 6
2. CONTACT INFORMATION 7
   2.1. Name of the Team 7
   2.2. Address 7
   2.3. Time Zone 7
   2.4. Telephone Number 7
   2.5. Facsimile Number 7
   2.6. Other Telecommunication 7
   2.7. Electronic Mail Address 7
   2.8. Public Keys and Encryption Information 8
   2.9. Team Members 8
   2.10. Other Information 8
   2.11. Points of Customer Contact 8
3. CHARTER 9
   3.1. Mission statement 9
   3.2. Constituency 9
   3.3. Sponsorship and/or Affiliation 9
   3.4. Authority 9
4. POLICIES 10
   4.1. Types of Incidents and Level of Support 10
   4.2. Co-operation, Interaction and Disclosure of Information 10
   4.3. Communication and Authentication 11
5. SERVICES 12
   5.1. Incident Response 12
      5.1.1. Incident Triage 12

I-TRACING ©2022 – Reproduction prohibited without explicit permission

5.1.2. Incident Coordination *12*
5.1.3. Incident Resolution *12*
5.2. PROACTIVE ACTIVITIES 12
6. INCIDENT REPORTING FORMS 13
7. DISCLAIMERS 14

I-TRACING ©2022 – Reproduction prohibited without explicit permission

1. Document Information

This document contains a description of the CERT I-Tracing in accordance with RFC 2350 specification. It contains basic information about the CERT I-Tracing, the services offered and their scope.

1.1. Date of Last Update

This is version 1.2, published on 7 December 2022.

1.2. Distribution List for Notifications

Changes to this document are notified to CERT I-Tracing constituency through closed channel.

1.3. Locations where this Document May Be Found

The current and latest version of this document can be found on I-Tracing's website at:

https://www.i-tracing.com/cert/

1.4. Authenticating this Document

This document has been signed with the PGP key of the CERT I-Tracing. The PGP public key, ID and fingerprint are available on I-Tracing's website at:

https://www.i-tracing.com/cert/

1.5. Document Identification

Refer to document details table.

I-TRACING ©2022 – Reproduction prohibited without explicit permission

2. CONTACT INFORMATION

2.1. Name of the Team

Computer Emergency Response Team of I-Tracing names:

- Long name: CERT I-TRACING
- Short name: I-CERT

2.2. Address

I-TRACING SAS

Tour Workstation

25 quai du Président Paul Doumer

CS30133

92408 Courbevoie Cedex

FRANCE

2.3. Time Zone

CET/CEST

2.4. Telephone Number

CERT I-Tracing main number available on French office hours: +33 1 70 94 69 90

2.5. Facsimile Number

Not available.

2.6. Other Telecommunication

CERT I-TRACING does not provide any other telecommunication channel outside its constituency.

2.7. Electronic Mail Address

CERT I-Tracing team can be contacted for any inquiry related to its constituency and services by e-mail: <cert@i-tracing.com>

I-TRACING ©2022 – Reproduction prohibited without explicit permission

2.8. Public Keys and Encryption Information

I-Tracing's CERT supports PGP/GnuPG for secure correspondences:

- Key ID: 0x3F9C1033457BC04A
- Fingerprint: A963 ED66 CE3A A4C8 3E74 487F 3F9C 1033 457B C04A

The public key is shared with CERT I-TRACING constituency. It can be retrieved from one of the usual public key servers.

2.9. Team Members

The identities of the members of the CERT I-Tracing team are not publicly available. They may be disclosed on a case-by-case basis on the grounds of need-to-know restrictions.

2.10. Other Information

General information about I-Tracing and the services provided by the company can be found on I-Tracing's website: https://www.i-tracing.com

2.11. Points of Customer Contact

The preferred method to contact the CERT I-Tracing is via e-mail at <cert@i-tracing.com>. Please use our public key to ensure confidentiality and integrity.

Urgent assistance needs may be reported by phone (Cf. §2.4 - Telephone Number).

I-TRACING ©2022 – Reproduction prohibited without explicit permission

3. CHARTER

3.1. Mission statement

The CERT I-Tracing is a private Computer Emergency Response Team. Its mission is to support its constituency community with reactive and proactive services in the field of Cyber Security by:

- Gathering, evaluating, and disclosing information on vulnerabilities and threats to relevant teams for detection and vulnerability management,
- Providing technical expertise on security-focused questions,
- Coordinating discussions with external entities on the subjects of threat intelligence and information sharing

3.2. Constituency

The primary constituency is composed of I-Tracing, its partners, and its customers.

3.3. Sponsorship and/or Affiliation

The CERT I-Tracing is part of I-Tracing, a company specialized in information security.

3.4. Authority

The CERT I-Tracing operates under the authority of I-Tracing or on behalf of its constituency when requested.

I-TRACING ©2022 – Reproduction prohibited without explicit permission

4. POLICIES

4.1. Types of Incidents and Level of Support

CERT I-Tracing addresses all types of information security incidents which occur in its constituency.

The level of support given by the CERT I-Tracing will vary depending on the size and severity of the incident, the type of constituent, the available CERT I-Tracing resources and the level of support requested by the constituent. Resources will be assigned according to the following priorities, listed in decreasing order:

- Incident response and assistance,
- Incident analysis and forensics,
- Malware analysis,
- Alerts and advisories,
- Threat intelligence analysis.

Additionally, the CERT I-Tracing can integrate with any other I-Tracing teams to assist the constituent on:

- Extensive security analysis for remediation,
- Long-term remediation and risk mitigation plan.

4.2. Co-operation, Interaction and Disclosure of Information

All Information related to incidents followed by CERT I-Tracing is kept confidential and any technical or contextual information is only disclosed with the approval of the affected organization.

However, the CERT I-Tracing is aware that cooperation is a key part of the CERT and CSIRT community. Thus, when mandated, CERT I-Tracing collects and enriches technical data to improve detection capabilities and capitalize on past incidents. Data is always anonymized before being shared to any internal or external party. CERT I-Tracing may share information with:

- I-Tracing Internal teams related to cyber defense activities
- Customers and partners, including external CSIRT and CERT teams and sharing communities
- Law enforcement and governmental agencies

All information is securely stored and shared on a need-to-know basis. Each element passes through an evaluation process to check if it is relevant for the other party and if its classification and diffusion policy is compatible. The diffusion policy respects the Information Sharing Traffic Light Protocol (TLP) and the tags as specified by the FIRST at: https://www.first.org/tlp/.

I-TRACING ©2022 – Reproduction prohibited without explicit permission

4.3. Communication and Authentication

The CERT I-Tracing 's preferred contact method is e-mail. For the exchange of sensitive material, please use the PGP key specified in section 2.8 to encrypt data. The CERT I-Tracing may also use other encryption methods on a case-by-case basis, for example when regulation requires specific encryption technologies.

I-TRACING ©2022 – Reproduction prohibited without explicit permission

5. SERVICES

5.1. Incident Response

CERT I-Tracing will assist its constituency in handling the technical and organizational aspects of security incidents. By default, assistance will be provided during the business hours specified in section 2.11. However, any constituent can ask for assistance on a 24/7 basis.

5.1.1. Incident Triage

- Investigation determining if the incident that occurred is technical or related to malicious activities
- Determination of the extent of the incident

5.1.2. Incident Coordination

- Constitution of the incident handling team and communication channels
- Coordination of early incident actions aiming at proof preservation and damage containment
- Qualification of the incident and onboarding of the appropriate team members (both from the constituent and CERT I-Tracing Group resources)

5.1.3. Incident Resolution

- Analysis of compromised systems
- Identification and elimination of causes of a security incident (user access, vulnerabilities, etc.)

5.2. Proactive Activities

- Warning and information services available to mailing lists diffused to the constituents
- On-demand information services and analyses
- Delivery of threat intelligence to CERT I-TRACING constituency and assistance in contextualization

The CERT I-Tracing also works with other I-Tracing services included in the following activities:

- Audit activities, notably post-compromise security audit
- Internal IT teams for assistance with information system operations and security models

I-TRACING ©2022 – Reproduction prohibited without explicit permission

6. INCIDENT REPORTING FORMS

No specific incident reporting form must be completed. Incident key points will be determined during the qualification phase following the qualification process in place in the CERT I-Tracing team.

I-TRACING ©2022 – Reproduction prohibited without explicit permission

7. DISCLAIMERS

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

I-TRACING ©2022 – Reproduction prohibited without explicit permission