Industrie Services Tertiaire

Cert-IST RFC-2350 (Description of services)

TLP	**[TLP: WHITE]** *TLP: WHITE information may be distributed without restriction, subject to copyright controls.*
Reference Cert-IST	CertIST-P-DS-18-0012-EN
Version	1.0
Date	December 17th, 2018

Table of contents

Version history

Version & Date	Author	Change description	Pages		
			Add.	Change	Remov.
1.0 17-Dec-2018	Ph. Bourgeois	Creation of the document	All		

1 ABOUT THIS DOCUMENT

Foreword: This document describes the Cert-IST services in compliance with the RFC 2350 document. RFC 2350 is an IETF Best Current Practice available at: https://www.ietf.org/rfc/rfc2350.txt

1.1 Date of Last Update

The current version of this document is version 1.0 and was released on December, 17th 2018.

1.2 Distribution List for Notifications

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

1.3 Location where this Document May be Found

The current version of this document is available on Cert-IST public web site, at the following location:
https://www.cert-ist.com/public/en/rfc2350

1.4 Authenticating this Document

This document has been signed with the Cert-IST **PGP key** and the signature file is available at the same location as the document itself.

Cert-IST's public PGP key is given at chapter 2.8 below.

2 CONTACT INFORMATION

2.1 Name of the Team

Short name: **Cert-IST**
Full name: **CERT for Industry Service and Tertiary sectors**

2.2 Address

To join the Cert-IST Steering Committee:

Cert-IST
3 quai du point du jour
92100 Boulogne Billancourt
FRANCE

To join the technical team:

Thales
Bâtiment Pastel – Site de Labège
290 allée du Lac
ZAC de l'Hers
31670 LABEGE
FRANCE

2.3 Time Zone

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

2.4 Telephone Number

+33 5 34 39 44 88

2.5 Facsimile Number

+33 5 34 39 44 89

2.6 Other Telecommunication

None available

2.7 Electronic Email Address

cert(at)cert-ist.com

2.8 Public Keys and Other encryption Information

Cert-IST PGP public Key information are:

- KeyID: 0x350A60BA
- Fingerprint: 6783 4DD2 6F22 A014 4CE9 7D42 B6BE A8FA 350A 60BA

Cert-IST's public PGP key is available at the following location:
https://www.cert-ist.com/public/en/ClePGP

2.9 Team Members

The team is composed of security experts who work full-time on Cert-IST activities.
Because of privacy concerns, we do not publish the names of our team members in public documents. Please contact us directly if you need more information.

2.10 Operating Hours

Cert-IST can be joined on business hours: Monday to Friday, 9:00AM to 6:00PM
Cert-IST is closed on French public holidays.

2.11 Additional Contact Info

The section "Contact the Cert-IST team" on our public web site provides advice to contact us:
https://www.cert-ist.com/public/en/contacts

3 Charter

3.1 Mission statement

Cert-IST is a private CERT dedicated to Companies belonging to the Industry, Service and Tertiary (I.S.T.) sectors. Its services are available to organisations that have subscribed to Cert-IST services, and such an organisation is called a Cert-IST Member.

Cert-IST missions are:

- To watch open and closed sources to be aware of new cyber vulnerabilities, threats and attacks,
- To inform Members for significant events in this field,
- To share threat information that members are willing to share with other Members,
- To be a relay between Members and security teams in the world,
- To provide support to its Members to deal with incident.

3.2 Constituency

The Cert-IST constituency is composed of all the organisations that subscribed to Cert-IST services (i.e. all the Members).

Current Members include companies from the following sectors: Aerospace, Bank, Defense Industry, Healthcare, Insurance, Oil & Gas, Telecom, Utilities, etc.

3.3 Sponsorship / affiliation

3.3.1 Cert-IST Sponsorship and funding

Cert-IST activities are funded by its Members.

The Cert-IST Members are united in a non-profit association (a French “Loi 1901” association). The Association’s Board is the Steering Committee that leads and reviews the activities of a technical team which performs the Cert-IST services.

The technical team is operated by THALES Group.

3.3.2 Organizations to which Cert-IST is affiliated

At the international level, Cert-IST is a member of FIRST organisation (www.first.org) since 1999.

At the European level, Cert-IST is an accredited member of the Trusted Introducer since March 2006 and participate to the TF-CSIRT which promote the collaboration between Computer Security Incident Response Teams (CSIRTs) in Europe.

At the French level, Cert-IST is a member of the French CERTs group: InterCERT-FR

3.4 Authority

Cert-IST is led by a Steering Committee composed with a set of Member organisation representatives.

Cert-IST services are performed by a technical team that are employees of the THALES Group.

4 Policies

To comply with the RFC-2350, we present the Cert-IST policies in the order defined by the RFC-2350 document (in sections 4.1 to 4.3). Other policies are presented after (section 4.4).

4.1 Types of Incidents and Level of Support

Cert-IST provides:

- incident coordination service (see § 5.1.2) for any cyber incident that affects one of its members. Anyone who is aware of a cyber-incident that might impact a Cert-IST member may contact Cert-IST to report this incident.

- incident resolution services (see § 5.1.3) to the Cert-IST members. Only members may ask for this service.

The level of support given will vary depending on the severity of the incident, the size of the user community affected, and Cert-IST resources at the time.

In addition to incidents (which are situations where an attack has occurred or is occurring), Cert-IST also addresses vulnerabilities in software or in infrastructures:

- The discoverer of a new vulnerability may report this vulnerability to Cert-IST, and Cert-IST will assist him to contact the affected vendor. This event will be treated through the incident coordination service (in conformance with the responsible disclosure policy described in chapter 4.4) even if the affected product does not belong to a Cert-IST member. See chapter 5.1.2 for further details.
- Cert-IST informs its members about new vulnerabilities through its pro-active services, as described in chapter 5.2.

Cert-IST operates within the current French legal framework.

4.2 Co-operation, Interaction and Disclosure of Information

To accomplish its mission and perform its services, Cert-IST regularly interacts with other organisations, such as other CERT or CSIRT teams, Vendors, vulnerability Reporters, etc.

Our first priorities are to preserve:

- The level of confidentiality assigned to information by its owner. We use “TLP” protocol (as define by FIRST: https://www.first.org/tlp/) to define information confidentiality.
- The privacy of personal information.

No sensitive information will be sent by Cert-IST to another party without a prior agreement of the information owner.

4.3 Communication and Authentication

In view of the types of information that Cert-IST deals with, telephones will be considered sufficiently secure to be used even unencrypted.

When sent on non-secure communication channel such as email, sensitive information is encrypted. Preferably, Cert-IST uses PGP or S/MIME to encrypt data. If this is not appropriate for the other party, other mechanisms can be used as well, e.g. symmetric encryption with a password key decided in advance.

To authenticate the messages it releases, Cert-IST uses:

- PGP to sign files,
- and S/MIME to sign emails.

4.4 Vulnerability responsible disclosure

This policy is followed by Cert-IST when Cert-IST is aware of a new security vulnerability that has not been publicly disclosed yet. This policy aims at ensuring security for Cert-IST constituency and at enabling Vendors to develop solutions quickly for their security problems.

- Cert-IST is committed to provide assistance, within its capabilities, to facilitate the dialogue between a **Reporter** (who discovered a new security vulnerability) and the **Vendor** of the solution affected by this vulnerability. The primary role of the Cert-IST is consequently to be a **Coordinator**, as defined in the RFC Draft **"Responsible Vulnerability Disclosure Process"** (published by IETF in February 2002). It may sometimes also act as Reporter. If resource constraints make Cert-IST unable to provide this coordination service, then it will inform the impacted parties and direct them to alternative solutions.

- Cert-IST undertakes to respect a grace period which is generally of 90 days before publishing its advisories. Thus during the discovery process of a new vulnerability, Cert-IST notifies the Vendor, making known to him the information that will be published, should no response be supplied at the end of the grace period. If the threat importance requires to shorten this delay, the various actors (specifically the Vendor) are informed. This grace period only concerns new vulnerabilities, which means vulnerabilities that have not already been published in a public forum (open mailing lists, public Web sites, etc...).

- During the Vendor notification period, Cert-IST undertakes to provide all necessary information to enable the Vendor to qualify the vulnerability: problem description, tested versions, code used and all technical information useful for the problem comprehension. The notification is generally made by email and the notification date is recorded.

- Except if the Reporter does not agree, Cert-IST indicates the Reporter name to the Vendor during the notification and to Cert-IST constituency when the advisory is released.

- Cert-IST policy will be enforced for all the Editors uniformly.

- Nevertheless, in case of big security risks, Cert-IST reserves the right to publish the information before or beyond the grace period; the decision to publish or not an advisory will always take into account **the interests in terms of security** of the various actors. Whenever possible, Cert-IST will propose a workaround to allow the users to protect themselves against the vulnerability exploitation.

5 Services

5.1 Incident Response

Cert-IST provides 2 major services in the field of Incident Response:

- Incident Coordination,
- Incident Resolution.

But before these services are performed, a first task is to perform:

- Incident Triage

5.1.1 Incident Triage

- Collect the information about the incident.
- Confirm that the described event is actually a cyber security incident and is related to a Cert-IST Member.
- Determine the severity of the incident (what is the impact) and its extent (how many computers are affected).
- Decide which type of service (coordination or resolution) should be triggered.

5.1.2 Incident Coordination

Cert-IST acts has a **Coordinator**, between a **Reporter** (who triggered the incident process) and **Third Parties** (who are the stakeholders involved in the resolution of the incident).

Except in case of vulnerability disclosure incident (which is covered below), Cert-IST performs this incident coordination service only if a Cert-IST Member is involved in the incident, either as a Reporter, or as an impacted Third Party. This means that:

- A Cert-IST member may request the Incident Coordination service to dialog about an incident with a set of Third Parties with the help of Cert-IST.
- A external Reporter may request the Incident Coordination service to dialog about an incident with Third Parties that are Members of Cert-IST

The role of Cert-IST is:

- To provide anonymity to the Reporter who wants to contact Third Parties anonymously,
- To provide assistance, within its capabilities, to facilitate the dialogue between the Reporter and the Third Parties.

Vulnerability disclosure incident: This incident coordination service also applies when somebody who has discovered a new vulnerability in a product, want to report it to the product vendor, through Cert-IST. In this case, Cert-IST will provide this service to any reporter and even if the affected product vendor is not a Cert-IST member. Please note that this service is assigned a lower priority that the other Cert-IST services, and could be delayed if no resource is available at this time to perform it.

5.1.3 Incident Resolution

Incident resolution service is available only for Cert-IST Members who subscribed the incident support service. The level of service provides by Cert-IST depends on the Member needs, and is define when the incident case is open. It could range from technical expertise on specific tasks (e.g. log analysis, forensic analysis, etc.) to incident response leading and management.

5.2 Proactive Activities

Cert-IST provides to its Members a set of **proactive Watch, Monitoring and Alert services**. This includes:

- Security advisories,
- Alerts,
- Attack datasheets.

5.2.1 Security advisories

Security advisories describe newly discovered vulnerabilities (and available solutions to fix them) for any product followed by the Cert-IST. These advisories are continuously enriched with minor or major updates. The latter typically occurs when attack programs (aka “exploits”) are released.

5.2.2 Alerts

Alerts are released to inform that an attack of a significant magnitude is imminent or already underway. They are typically issued when an attack spreads over the Internet. There are three levels of alert: **yellow** alert, **orange** alert and **red** alert.

5.2.3 Attack datasheets

Attack datasheets describe the major attack seen, for recurring threats (MalSpam, Exploit-Kit, Ransomware), as well as cyber-espionage attacks (APT). In addition to a general description, the attack datasheet includes a description of the TTP Tactics Techniques and Procedures) and IOCs (Indicator of Compromise).

6 Incident Reporting Forms

An incident report form is available on line at:
https://www.cert-ist.com/public/en/declarerIncident

A vulnerability report form is available on line at:
https://www.cert-ist.com/public/en/declarerVulnerabilite

7 Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, Cert-IST assumes no responsibility for errors or omissions, or for damages resulting from the use of the Information it provides.

End of document