CERT Description for Thales CERT RFC 2350

Document Control

Approval

	Name	Date
Prepared by	Julien Vignolles	15/Sep./2016
Approved by	Didier Espinet	16/Sep./2016

History

Revision	Author	Date	Modification
1.0	Julien Vignolles	15/Sep./2016	Initial version
1.1	Julien Vignolles	06/Apr./2017	User modifications, working time
1.2	Julien Vignolles	15/Jun./2017	Adding PGP keys information
1.3	Julien Vignolles	07/Aug./2017	Typo fixes
1.4	Julien Vignolles	16/Aug./2017	Key ID updated
1.5	Julien Vignolles	28/Aug./2017	Typo fixes
1.6	Julien Mongenet	12/Jun./2018	Team and Roles modification
1.7	Rita Barakat	09/Apr./2019	Updated Gemalto to Thales
1.8	Rita Barakat	15/Nov/2019	Updated CERT members and PGP keys
1.9	Rita Barakat	18/Dec/2019	Updated CERT members roles

Table of Contents

1. About this document 4
1.1. Date of last update 4
1.2. Distribution list for notifications 4
1.3. Location where this document may be found 4
1.4. Authenticating this document 4
2. Contact information 5
2.1. Name of the team 5
2.2. Address 5
2.3. Date of establishment 5
2.4. Time zone 5
2.5. Telephone number 5
2.7. Other Telecommunication 5
2.8. Electronic email address 5
2.9. Public keys and other encryption information 5
2.10. Team members 5
2.11. Points of customer contact 6
3. Charter 7
3.1. Mission statement 7
3.2. Constituency 7
3.3. Sponsorship and/or affiliation 7
3.4. Authority 7
4. Policies 8
4.1. Types of incidents and level of support 8
4.2. Co-operation, interaction and disclosure of information 8
4.3. Communication and authentication 8
5. Services 9
5.1. Incident Response 9
5.1.1. Incident triage 9
5.1.2. Incident coordination 9
5.1.3. Incident resolution 9
5.2. Proactive activities 9
6. Incident reporting forms 10
7. Disclaimers 11

1. About this document

This document contains the description of Thales CERT according to the RFC 2350. It provides information about Thales CERT Team, communication channel and services.

1.1. Date of last update

This is the v1.8 version released on November, 15th 2019.

1.2. Distribution list for notifications

Distribution list for notifications changes related to this document are not distributed by a mailing list, or any other mechanisms.

1.3. Location where this document may be found

The current version of this Thales CERT description is available on PDF format on the Thales website.
https://www.gemalto.com/CSIRT

1.4. Authenticating this document

These documents have been signed with the Thales CERT PGP key. The signatures are available on our website, under:
https://www.gemalto.com/CSIRT

2. Contact information

2.1. Name of the team

The registered name of the team is **Thales CERT** and the acronym is "**THA-CERT**".

2.2. Address

Thales CERT
CERT – PO 63
525 Avenue du Pic de Bertagne – BP100
13881 GEMENOS Cedex – France

2.3. Date of establishment

Thales CERT was established in October 2013.

2.4. Time zone

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

2.5. Telephone number

+33 4 42 36 50 00 (Standard ask for CERT Team)

2.6. Other Telecommunication

None available

2.7. Electronic email address

All incident reports should be submitted to <cert(at)thalesgroup.com>.

2.8. Public keys and other encryption information

Thales CERT PGP Key information are:

KeyID: 0x026A9D84
Fingerprint: **ECDF D820 845A AACD 9627 627E 4C52 0648 026A 9D84**
The public key and its signature can be found at the usual large public key servers, or on Thales CERT information page: https://www.gemalto.com/CSIRT (should be updated soon)

2.9. Team members

CERT Coordination is performed by Julien Mongenet. All team members contact information are listed below:

Name	***Email address***	***Key ID***	***Role***
Didier Espinet	didier.espinet(at)thalesgroup.com	0xBFC15E46	Representative
	Fingerprint: **6380 F846 C2E3 2F7D B7C2 EB96 F956 D4A8 BFC1 5E46**		
Julien Mongenet	julien.mongenet(at)thalesgroup.com	0xCA337BD4	Head of CERT
	Fingerprint: **9FC1 9413 9E1F 653F 2D3E 863C 09FC A0B5 CA33 7BD4**		
Rita Barakat	rita.barakat(at)thalesgroup.com	0xB523440E	Core Team
	Fingerprint: **6B14 D044 FBC0 29C3 0E49 B4D1 A524 54E7 B523 440E**		
Sebastien Schmitt	sebastien.schmitt(at)thalesgroup.com	0x3D9B1B66	Core Team
	Fingerprint: **C948 4E73 50CF F199 17C9 CE04 76DB E724 3D9B 1B66**		
Alexandre Aumoine	Alexandre.aumoine(at)thalesgroup.com	0x7864FACC	Core Team
	Fingerprint: **D21E EFEE 79C0 43F9 B7EC 8EFA 4192 1851 7864 FACC**		

2.10. Points of customer contact

In case of security incident, in addition of regular Thales point of contact (Sales, support team), customers could submit incident report to <cert(at)thalesgroup.com>.

3. Charter

3.1. Mission statement

The Thales CERT's activities are non-profit and fully financed by Thales. The purpose of Thales CERT is to:

- Handle, contain, investigate and resolve serious computer security incident which can affect Thales' assets and interests including Thales' Customers, Employees, Partners and Shareholders, according the laws and regulations that may apply.
- Prevent and anticipate Computer Security Incidents by implementing adequate processes, tools, policies to improve the reactivity in case of an incident.
- Supports at a corporate level the crisis cell and manage the security implication of a crisis
- Provide information, expertise, assistance and tools to Thales to proactively reduce the risk of such incidents.

3.2. Constituency

The Thales CERT organization is divided into four constituencies: Infrastructure Technology, Operated Services, Manufacturing and Corporate Security, with all necessary Incident Response and Management activities. Thales CERT aims at providing cyber security expertise, defense, and efficient reactivity to protect our customers, shareholders and employees.

3.3. Sponsorship and/or affiliation

Thales CERT is a private CERT in the industrial sector. It is owned, operated and financed by Thales.
It maintains relationships with different CERTs in Europe and beyond.
Thales CERT is registered on Trusted Introducer since October 2016.
https://www.trusted-introducer.org/directory/teams/gto-cert.html

3.4. Authority

Thales CERT operated under the auspices of, and with the authority delegated by the Chief Security Officer of Thales. THA-CERT strives to work cooperatively with IT Managers, System Administrators, SOC, Datacenter Security Officer, Solution Security Officer and Security Site Managers to avoid authoritarian relationship whenever possible. However, under circumstances, Thales CERT will appeal to CIO, (S)VP, EVP to exert its authority directly or indirectly.

4. Policies

4.1. Types of incidents and level of support

Thales CERT manages all types of computer security incident which occur, or threaten to occur, in the different constituencies mentioned above. All confirmed incidents are qualified by type of incident and severity (Low, Medium, and High) according to our severity matrix. In all cases responses will be made according the priority and severity of incident reported.

Note that no direct support is given to end users; they are expected to contact their Service Desk or Local IT Managers, Security Site Managers for assistance.

4.2. Co-operation, interaction and disclosure of information

Thales CERT develops and maintain communication channels with other CERTs through official communication ways and specific tools (MISP).

THA-CERT protects sensitive information (business, privacy) in accordance with relevant law and regulations that may apply of the different countries where Thales is present.

THA-CERT applies Light Traffic Protocol (TLP) when sharing information with team that support it. TLP classification is based on the global Thales Document Classification Policy.

4.3. Communication and authentication

In view of the types of information that THA-CERT deal with, telephone will be considered sufficiently secure to be used even unencrypted. However, THA-CERT will refrain exchanging too sensitive detailed information through telephone and ask counterparts to proceed with encrypted emails.

Unencrypted e-mail must be used to submit non-sensitive information, and will not be considered as secure.

To submit high-sensitive data we encourage the use of the encryption means such as PGP Key (external) or X.509 cryptography for internal e-mail. PGP key information is described above.

All external e-mail coming from Thales CERT is digitally signed PGP or X.509.

5. Services

5.1. Incident Response

THA-CERT is informed about all security incident that occurs in the different constituencies. According to the extent of the security incident, THA-CERT takeover the lead and manages containment, analysis and recommend remediation actions with the support of system administrators and business managers.

5.1.1. Incident triage

- Confirm If the security event report is a relevant security incident
- Perform quick assessment (type, constituency, severity) of security incident confirmed and escalated incident

5.1.2. Incident coordination

- Determine the priority of the incident
- Take and push to constituency affected a first level of containment
- Manage the incident on THA-CERT side (investigations, reporting) and liaise with local security actors
- Communicate with other external parties if relevant
- Publish internal bulletin (Security Alert, Vulnerability information) to security coordinators & actors within the different constituencies.
- Attend to crisis meeting and liaise with legal, communication and business for technical security investigation that are in progress

5.1.3. Incident resolution

- Lead technical investigation, this could be done by local people but reported to CERT Core Team.
- Provision IOCs and liaise with SOC Team to detect and block abnormal activities
- Tune first level of containment according to the extent of the incident
- Determine the root causes and request Fix/Patch/Hardening of the affected systems
- Collect and store evidences, to start legal actions if necessary.
- Follow remediation and recovery activities until security risk dropdowns.
- Recommend security improvements to system administrators and business managers (Post-Mortem)

5.2. Proactive activities

Regarding THA-CERT resources, we coordinate and maintain the following services

- Threat notification
- Cybersecurity support and advices
- Vulnerability survey tool
- Training and educational services

6. Incident reporting forms

To ease security event reports (Incident, Vulnerability), you can directly send an email to <cert(at)thalesgroup.com> with an explicit subject describing the issue encountered. In addition, for emergency notification, we encourage you to prefix your email's subject with [URGENT]. According to the sensitivity of the information, prefer to cipher and digitally sign your email.

7. Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, Thales assumes no responsibility for errors or omissions, or for damages.

END OF DOCUMENT