Thales CERT

RFC 2350

version 3.0

Description of Services

TLP:CLEAR

Table of Contents

Version History

Version	Date	Change description	Pages		
			Added	Change	Removed
1.0	15-Sep-2016	Document creation	All		
1.1	06-Apr-2017	User modification, working time		§2.9 §2.10	
1.2	28-Aug-2017	Adding PGP keys information, team modification	§2.8	§2.9	
1.3	12-Jun-2018	Team and roles modification		§2.9 §3.1	
2.0	18-Dec-2019	Updated Gemalto to Thales, updated CERT members, members roles and PGP keys		§2.8 §2.9	
2.1	08-Oct-2021	GDPR compliance		§2.9	
3.0	01-Jun-2025	Updated all document		All	

Section

1

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 service.

1.1. Date of last update

This is the 3.0 version released on June 1st 2025.

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 published in PDF format on Thales' public website, at the following location: https://www.thalesgroup.com/en/global/group/cert.

1.4. Authenticating this document

This document has been signed with the PGP key of **Thales CERT**.

Thales CERT's PGP key is given at chapter 2.7.

1.5. Document validity

Title	THA-CERT RFC 2350
Version	3.0
Document Date	2025-06-01
Expiration	this document is valid until superseded by a later version.

Section

2

2. Contact information

2.1. Name of the team

The registered name of the team is **Thales CERT** (*Computer Emergency Response Team*) and the acronym is “**THA-CERT**”.

The team may also be found under the name **Thales PSIRT** (*Product Security Incident Response Team*) or the acronym “**THA-PSIRT**” in the event of products’ or solutions’ security incidents.

2.2. Address

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

2.3. Time zone

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

2.4. Telephone number

+33 1 73 17 04 00 (24/7 – *refer to paragraph 2.9*).

2.5. Facsimile number

Not available.

2.6. Electronic email address

If you need to notify us about an **information security incident** or a **cyber-threat** targeting or involving **Thales Group**, please contact us at <**cert(*at*)thalesgroup[.]com**>.
In case you need to notify us about a **Thales product or solution vulnerability** or a **data leak** involving **Thales Group**, please contact us at <**psirt(*at*)thalesgroup[.]com**>.

2.7. Public keys and other encryption information

2.7.1. Thales CERT

Thales CERT PGP Key information are:

User ID	<cert(*at*)thalesgroup[.]com>
Key ID	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.thalesgroup.com/en/global/group/cert.

2.7.2. Thales PSIRT

Thales PSIRT PGP Key information are:

User ID	<psirt(*at*)thalesgroup[.]com>
Key ID	0x8448AE39
Fingerprint	**FC3C 4520 576E C756 AE73 0030 5369 49C4 8448 AE39**

The public key and its signature can be found at the usual large public key servers, or on Thales PSIRT information page: https://www.thalesgroup.com/en/global/group/psirt.

2.8. Team members

The team is composed of cyber security experts who work full-time on activities related to security incidents response involving Thales Group.
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.

2.9. Other information

2.9.1. Additional contact info (outside operation hours)

In case of security incident, please apply the following recommendations:

- if the security incident is not sensitive, it will be managed during operating hours (*see section 2.9.2*). Please send the incident's details to:
  - <cert(*at*)thalesgroup[.]com>, or
  - <psirt(*at*)thalesgroup[.]com>.
- if security incident is sensitive, call the telephone number detailed in section 2.4 and send the incident's details using the above appropriate email addresses, and:
  - Thales CERT PGP key (*see section 2.7.1*), or
  - Thales PSIRT PGP key (*see section 2.7.2*).

2.9.2. Operating hours

You can contact Thales CERT and Thales PSIRT during business hours: Monday to Friday, 9:00AM to 6:00PM CET/CEST.

2.9.3. Date of establishment

Thales CERT was established in **October 2013**, and Thales PSIRT in **April 2019**.

Section

3

3. Charter

3.1. Mission statement

Thales CERT's activities are non-profit and fully financed by Thales.

In addition to the customary missions attributed to a **CERT**, Thales CERT closely collaborates with Thales PSIRT (*Product Security Incident Response Team*) and contributes to activities related to both **PSIRT** and **CTI** (Cyber Threat Intelligence).

The purpose of this team is to:

- **Handle**, **contain**, **investigate** and resolve cybersecurity incidents that can affect Thales' assets, products, solutions and interests according to the constituency (*see section* 3.2).
- Manage the **lifecycle of vulnerabilities** reported in Thales' products and solutions, and **coordinate remediation** activities with internal development teams.
- **Support** at a corporate level the **crisis cells** and manage the security implication of a crisis.
- **Prevent** and **anticipate** cybersecurity incidents by implementing adequate processes, tools and policies to improve the reactivity in the event of a cybersecurity incident.
- **Monitor** the **cyber threat landscape** (geopolitical, emerging threats, adversary tactics, sector-specific risks, vulnerabilities, threat actors, …) that could affect the security posture of Thales operations or sectors of activity.
- **Deliver actionable intelligence** to inform defensive measures, enrich incident investigations, and support risk management decisions.
- **Provide information**, **expertise**, **assistance** and **tools** to Thales to proactively reduce the risk of such incidents.

3.2. Constituency

Thales CERT constituency is composed of all Thales Group companies and subsidiaries.

This scope extends to Thales' Customers, Employees, Partners and Shareholders, according to the laws and regulations that may apply

Thales CERT aims at providing cyber security expertise, defense, and efficient reactivity to protect its 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 Group.
It maintains relationships with different CERTs in Europe and beyond.
Thales CERT maintains strong ties with the broader incident response and cybersecurity community.

At the **international level**, Thales CERT is a member of the FIRST organization (*Forum of Incident Response and Security Teams*) since 2023, which fosters trusted collaboration and information sharing among CSIRTs worldwide. Thales CERT is also a member of A-ISAC (*Aviation Information Sharing and Analysis Center*), which facilitates threat intelligence sharing and collaboration across the global aviation industry to enhance sector-wide cybersecurity.
At the **European level**, Thales CERT is an accredited member of the Trusted Introducer community since 2016 and formally accredited since 2017. This community promotes cooperation and best practices among European CSIRTs.
At the **national level**, Thales CERT is a member of InterCERT France, the French community of recognized CSIRTs coordinated by CERT-FR, since 2017.

On the other hand, Thales PSIRT is part of the CVE Program (since October 2021) and part of GCVE Program (as GNA, since May 2025 - *https://gcve.eu/dist/gcve.json*).

These affiliations enable Thales CERT and Thales PSIRT to maintain strong ties with trusted peers, **enhance its threat intelligence capabilities**, and **align its practices** with international standards.

3.4. Authority

Thales CERT operates under the authority of the **Group CISO** (*Chief Information Security Officer*) of Thales.

Thales CERT holds a **formal written mandate** signed by Senior Executive Vice Presidents of Thales. This document officially authorizes Thales CERT's incident response activities and provides the legitimacy and support required to act across the organization.

Thales CERT is recognized as the **central authority** for cybersecurity incident coordination across the Group. The team works cooperatively with local security representatives, SOC (*Security Operation Center*) engineers, IS/IT teams, Product and Solution Security Officers, etc.

Section

4

4. Policies

4.1. Types of incidents and level of support

Thales CERT addresses all types of cybersecurity incidents and threat scenarios that may impact or already impacts **Thales' information systems, products, solutions, or employees**.
This includes both **confirmed incidents** and **early warning signs** identified through internal and external monitoring, threat intelligence, or threat hunting.

Thales CERT manages the types of events described in section 5.

All reported or detected incidents are classified based on their **type** and **severity** (Low, Medium, High, Critical), following an internal standardized **severity engagement matrix**.
Response prioritization is based on the **severity**, the **business impact**, and the **criticality** of the assets involved.

For incidents **beyond the scope** of existing categories, Thales CERT applies a default "**best effort**" response model, while continuously updating its detection and classification capabilities.

End-users are not supported directly. They are expected to report incidents to their local IT support, Service Desk, or Security Site Manager, who may escalate to Thales CERT when necessary.

4.2. Co-operation, interaction and disclosure of information

Thales CERT maintains operational relationships with national and international CSIRTs, industry ISACs, vendors, and trusted partners for the purpose of incident coordination and threat intelligence sharing.

Any information shared by or with Thales CERT is protected in accordance with applicable laws and regulations, as well as Thales internal confidentiality and classification rules.

When sharing externally, the CERT uses the latest version of TLP (*Traffic Light Protocol*) and PAP (*Permissible Actions Protocol*) defined by the FIRST, to define the permitted level of redistribution.

4.3. Communication and authentication

Thales CERT supports both **PGP** and **X.509** for secure email communication (*see section 2.7*). All outbound messages containing **official statements** or **sensitive information** should be **digitally signed**, and encryption is **strongly recommended** for any **confidential exchanges**.

Unencrypted emails may be used for **general** or **non-sensitive** communications. It cannot be considered as secure. **Sensitive technical details** (such as vulnerability reports) or **incident data** (such as IPs) should only be shared via **encrypted channels**.

Thales CERT may use telephone for urgent matters but any sensitive information shall be transmitted by encrypted email.

All shared information is classified according to the Traffic Light Protocol (TLP) when interacting with trusted third parties and aligned with Thales's internal information protection policies. By default, without any data classification nor encryption, Thales CERT will consider the shared information as TLP:GREEN and PAP:GREEN.

4.4. Vulnerability Responsible Disclosure

Thales PSIRT supports and promotes responsible vulnerability disclosure to ensure the security of Thales products and services and to protect its customers, users, and ecosystem.

The Product Security Incident Response Team (PSIRT) **coordinates** the intake, **triage**, and **remediation** of reported vulnerabilities, in collaboration with relevant internal stakeholders.

Thales PSIRT also acts as an official **CNA** (*CVE Numbering Authority*), allowing it to **assign CVE identifiers** to confirmed vulnerabilities in Thales' products and solutions.

Thales encourages researchers, partners, and any external parties to report potential vulnerabilities in a secure and responsible manner. Reports should be submitted via email to <psirt(*at*)thalesgroup[.]com>, using PGP encryption where necessary (*see section 2.7.2*).

Thales PSIRT follows recognized principles of coordinated responsible disclosure, including case-by-case evaluation, embargo periods, and secure handling of sensitive information.

For complete details on Thales's responsible disclosure process, visit the official policy page: https://www.thalesgroup.com/en/global/group/psirt.

Section

5

5. Services

The core mission of Thales CERT is to **reduce cybersecurity risk** across Thales, through **coordinated incident response**, **actionable intelligence**, and **proactive defense**.

To fulfill this mission, Thales CERT provides a comprehensive set of services, including real-time support during incidents, structured coordination with stakeholders, and continuous improvement activities to strengthen the Group's cyber resilience.

5.1. Incident Response

Thales CERT is informed of any cybersecurity incident or suspected activity that may significantly impact Thales' information systems, products, or services. It **coordinates** the technical response, **contributes** to investigations, and **leads** incident handling when necessary.

As part of its missions, Thales CERT supports **crisis management** by driving **containment**, **analysis**, and **remediation** activities.

Working in close collaboration with internal stakeholders (*as described in section 3.2*), Thales CERT ensures that all **technical aspects** of an incident are **addressed effectively**.

5.1.1. Incident triage

- **Assess** whether the report describes a valid security incident;
- Classify the incident by **type**, **severity**, and **affected constituency**, based on the internal **severity engagement matrix** (*see section 4.1*);
- **Prioritize** incidents based on urgency and potential business risk;
- **Correlate** reports with ongoing investigations or known threat activity;
- **Determine** if immediate containment actions are needed.

5.1.2. Incident coordination

Thales CERT coordinates the technical response to security incidents by:

- **Determining incident priority** and initiating **first-level containment** actions;
- **Coordinating** with affected internal stakeholders, including IT, SOC, product teams, and site security actors;
- **Coordinating** products and solutions related **vulnerability reports** with internal engineering teams and external reporters, in accordance with responsible disclosure principles, through the PSIRT's missions;
- **Interfacing with external parties** (e.g., vendors, partner CSIRTs, or regulators), when cross-boundary coordination is needed;
- **Categorizing** and **managing** incident-related **information** in line with Thales' information disclosure policy;
- **Participating in crisis meetings** and ensuring alignment with legal, communication, and business stakeholders;
- **Issuing internal alerts**, **advisories**, or **vulnerability bulletins** to inform and support the constituencies involved.

5.1.3. Incident resolution

Thales CERT contributes to incident resolution by coordinating technical response activities and supporting stakeholders in restoring secure operations. This includes:

- **Leading** or **supporting technical investigations** in collaboration with local teams;
- **Sharing Indicators of Compromise** (IOCs) and working **with SOC teams** to **improve detection**;
- **Collaborating with IS/IT** and **business teams** to **block malicious activity**;
- **Adjusting containment measures** as the situation evolves;

- **Identifying root causes** and **recommending appropriate corrective actions** (*e.g., patching, hardening*);
- **Supporting evidence collection** and **preservation** in case legal action is required;
- **Following-up on remediation** and **recovery efforts** until the threat is neutralized;
- **Providing post-incident recommendations** to strengthen security posture and prevent recurrence;
- **Assigning and publishing CVE identifiers** for confirmed vulnerabilities affecting Thales' products or solutions.

5.2. Proactive activities

In addition to its incident response capabilities, Thales CERT provides a range of proactive services aimed at strengthening the cybersecurity posture of the Thales Group. These services help anticipate threats, improve awareness, and reduce the likelihood or impact of incidents.

The team's proactive services include:

- **Cyber Threat notification**: disseminating timely alerts towards Thales' constituency, on emerging threats, campaigns, and vulnerabilities, that could impact Thales;
- **Vulnerability surveillance**: operating and maintaining a vulnerability survey tool to identify and monitor known and highly impacting weaknesses across Thales' systems;
- **Threat Intelligence surveillance**: enriching awareness with geopolitical and sectoral threat intelligence;
- **Cybersecurity advisory services**: providing expert guidance to technical and business teams on risk mitigation and best practices;
- **Training and awareness**: delivering educational content, workshops, and technical sessions to improve incident preparedness and cyber hygiene;
- **Team expertise and continuous development**: ensuring the ongoing technical proficiency of its members through regular participation in advanced cybersecurity training (*e.g., SANS, FIRST, etc.*), conferences, pursuit of professional certifications, and active involvement in cyber crisis simulations and internal exercises;
- **Threat hunting**: conducting proactive threat hunting activities in coordination with SOCs to detect undetected threats, anomalous behavior, and early-stage attack indicators across Thales' environments.
- **Monitoring of public data leaks**: monitoring publicly available sources, leak sites, and dark web channels to identify potential data exposures or leaks involving Thales' assets, credentials, or sensitive information.

These services are adapted to resource availability and evolving threat landscapes and are delivered in alignment with the Group's cybersecurity governance.

Section

6

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.

Thales CERT does not currently provide a generic public incident reporting form. Security incidents and vulnerabilities should be reported via email to the appropriate contact point:

- For incidents involving information systems or infrastructure: <cert(at)thalesgroup[.]com>;
- For products or services related vulnerabilities, responsible disclosure, or business data leaks: <psirt(at)thalesgroup[.]com>;
- For suspected fraud attempts: Thales Fraud Reporting Form.

To support efficient handling, the email should include as much relevant information as possible. Please include, where applicable:

- Date and time of the incident (specify time zone);
- Contact details of the reporting party;
- Summary and context of the issue;
- Estimated impact or risk;
- Source/Destination IPs, ports, and protocols (if relevant);
- Email headers or message samples (in case of phishing or abuse reports);
- Logs or technical evidence in a common format (if available).

If the report is **sensitive**, we strongly recommend using **encryption** (PGP) and digital signatures. For urgent notifications, please prefix the subject line with [URGENT].

Section

7

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