CSIRT DESCRIPTION FOR TCS-CERT RFC2350

TCS-CERT

Reference	TCS-CERT-RFC2350
Originator	TCS-CERT
Audience	THALES CYBER SOLUTIONS | EXTERNAL
Sharing level	TLP: CLEAR
Classification	PUBLIC

Document Versioning

Authoring

	Name
Verified by:	Lionel THONNATTE

Approval

	Name	Date
Approved by:	Fabien BERNARD	October 14, 2025

Copyright © 2025 – Thales Cyber Solutions. All rights reserved

Preparation & History

Version	Date	Author	Description
1.42	13/10/2025	Emmanuelle VANCRAEYENEST	User update
1.41	28/07/2025	Paul JUNG	Contact, email, link modifications
1.40	02/07/2025	Lucas JOBLIN	emails modifications
1.39	01/07/2025	Paul JUNG	User update
1.38	15/04/2025	Paul JUNG	User update
1.37	28/03/2025	Abdulsamet AKKUS	Links /emails modifications
1.36	05/03/2025	Dorian RETTER	Users Update (Senegal only)
1.35	29/01/2025	Paul JUNG	Users Update and name change
1.34	27/12/2024	Dorian RETTER	Users update
1.33	04/10/2024	Paul JUNG	Users update
1.32	02/05/2024	Arnaud GARRIGUE	Users update
1.31	22/03/2024	Arnaud GARRIGUE	Modified Suricate Incident handlers
1.30	09/02/2024	Dorian RETTER	Migration of Excellium Belgium to thalegroup.com domain
1.29	17/01/2024	Camille BOUR	Users update
1.28	03/11/2023	Camille BOUR	Users update
1.27	22/09/2023	Camille BOUR	Users update
1.26	01/09/2023	Camille BOUR	Users update
1.25	31/08/2023	Camille BOUR	Users update
1.24	28/06/2023	Lola GEROME	Users update
1.23	15/05/2023	Lola GEROME	Users update
1.22	27/04/2023	Lola GEROME	Users update
1.21	22/11/2022	Lola GEROME	Users update
1.20	15/04/2022	Dorian RETTER	Users update and review
1.19	22/12/2021	Paul JUNG	Users modification
1.18	17/09/2021	Razvan URSU	Users modification
1.17	17/08/2021	Paul JUNG	Users modification
1.16	26/05/2021	Paul JUNG	User modification
1.15	13/11/2020	Paul JUNG	User modification
1.14	15/10/2020	Paul JUNG	User modification

1.13	09/06/2020	Mathieu BAEUMLER	User modification
1.12	16/03/2020	Paul JUNG	User modification.

Initial Version

1.0	11/09/2014	Paul JUNG	Initial version.

Distribution List

Version	Company	Name
1.41	N/A	Public document

COPYRIGHT NOTICE AND CONFIDENTIALITY STATEMENT

Copyright © 2013-2025 by Thales Cyber Solutions Luxembourg S.A. & Thales Cyber Solutions Belgium S.A. or its affiliates and/or licensors. All rights reserved.

This document may contain confidential information about Thales Cyber Solutions Luxembourg S.A. & Thales Cyber Solutions Belgium S.A., its affiliates and/or licensors and their respective businesses, business partners and/or customers, all of which is provided in confidence and may be used by the intended recipient only for the sole purpose of the adjudication of the proposal.

It must not be used for any other purpose. Copies of this document may only be provided, and disclosure of the information contained in it may only be made to employees of the intended recipient connected with the negotiations and its named professional advisors who acknowledge its confidential status.

Any recipient must not to disclose this information, either wholly or in part, to any other party without prior permission in writing being granted by Thales Cyber Solutions Luxembourg S.A., Thales Cyber Solutions Belgium S.A. or any entity controlled by, controlling, or under common control with Thales Cyber Solutions Luxembourg S.A. or Thales Cyber Solutions Belgium S.A..

About this document.

Date of last update

This is the 1.42 version released on the 13th of October 2025.

Distribution List for notifications

Changes to this document are not distributed by a mailing list, RSS or any other mechanism. Please address any specific questions or remarks to TCS-CERT e-mail address (see chapter *Electronic mail address*)

Locations where this document may be found

The current version of this CSIRT description document is available in pdf format in the document section on the TCS-CERT WWW site. At the following URL:

https://cds.thalesgroup.com/sites/default/files/2025-07/CSIRT-RFC2350.pdf

Please make sure you are using the latest version.

Authenticating this document

These documents have been signed with the TCS-CERT's PGP key. The main signature is available on our website, under:

https://cds.thalesgroup.com/sites/default/files/2025-07/CSIRT-RFC2350.pdf.asc

Contact Information

Name of the team

“TCS-CERT”: Thales Cyber Solutions Customer’s CSIRT of

- Thales Cyber Solutions Luxembourg S.A.
- Thales Cyber Solutions Belgium S.A.

This team was named CERT-XLM before January 2025.

Addresses

The primary correspondence address is the Luxembourgish one.

TCS-CERT
Thales Cyber Solutions Luxembourg
5 rue de Goell
L-5326 Contern
Luxembourg

Thales Cyber Solutions Belgium
Orion Bldg, Belgicastraat 13
B-1930 Zaventem
Belgium

Timezone

CET / CEST

- GMT+01:00 in wintertime (from last Sunday in November to last Sunday in March).
- GMT+02:00 during summertime (from last Sunday in April to last Sunday in October).

Telephone number

- +352 262 039 64 708 TCS-CERT direct number (24/7).
- +352 661 348 273 Thales Cyber Solutions Luxembourg and Belgium CSOC (24/7).

Facsimile number

Non available.

Other Telecommunication

Non available.

Electronic mail address

All incident reports should be submitted to <**emergency(at)tcs-cert.com**>.

The team may be contacted at <**team(at)tcs-cert.com**>. This email alias relays emails to the human(s) on duty for the TCS-CERT.

Public keys and other encryption information

The TCS-CERT <**team(at)tcs-cert.com**> has a PGP key, with the KeyID **0xD74E5AC0** the related fingerprint is **8D78D1A67F2BAFDE41B74DBA67B311E5D74E5AC0**.

The Incident mailbox <**emergency(at)tcs-cert.com**> has the key PGP, with the KeyID **0x42662EFE**, the related fingerprint is **F27E7CE46E424205A68F2B9F4F753C7942662EFE.**

The public key and its signatures can be found at the usual large public key servers, or on TCS-CERT web site:

- for <**team(at)tcs-cert.com**>, under:
    - https://cds.thalesgroup.com/sites/default/files/2025-07/TCS-CERT_PKEY.asc
- for <**emergency(at)tcs-cert.com**>, under:
    - https://cds.thalesgroup.com/sites/default/files/2025-07/EMERGENCY_PKEY.asc

Each TCS-CERT team member also has a nominative OpenPGP public key.

Team members

CERT coordination will be performed by **Fabien BERNARD**. All team members, along with their areas of expertise and contact information, are listed below:

Luxembourgish Core Team

Name	Email	KeyID	Role
Amine GHARBI	mohamedamine.gharbi(at)thalesgroup.com	0xEB670867	Incident handler
	Fingerprint	B56D01293A680CC01FEC5E951BA330A4EB670867	
Fabien BERNARD	fabien.bernard(at)thalesgroup.com	0xC0516A33	Coordinator
	Fingerprint	0B0C7EC64AA0B6BC7623BBBBF2C1E828C0516A33	
Abdulsamet AKKUS	abdulsamet.akkus(at)thalesgroup.com	0x721C9AF7	Incident handler
	Fingerprint	74A254AD4DF92E45B54D6293A0D95FE8721C9AF7	
Lucas JOBLIN	lucas.joblin(at)external.thalesgroup.com	0x5DCE39D7	Incident handler
	Fingerprint	AEFF5E34F6F1396F34188079F4DC73535DCE39D7	
Alexis DE BRITO	alexis.debrito(at)thalesgroup.com	0x1F7FD6D2	Incident handler
	Fingerprint	0A487E9A720C3816EF8B6E77B53F6C9D1F7FD6D2	
Nolan CORBELLARI	nolan.corbellari(at)thalesgroup.com	0x8C48665C	Incident handler
	Fingerprint	ADB35386550E9E4747F80FB9944BEB778C48665C	
Steven SMILA	steven.smila(at)thalesgroup.com	0x8F984A8F	Incident handler
	Fingerprint	131383BBF51336075D71694061941C2F8F984A8F	
Emmanuelle VANCRAEYENEST	emmanuelle.vancraeyenest(at)thalesgroup.com	0x2FD5DBF2	Project Manager
	Fingerprint	31A23A83C66B986F23FE283189F810A52FD5DBF2	
Steve GELHAUSEN	steven.gelhausen(at)thalesgroup.com	0x3F378983	Incident handler
	Fingerprint	27CC40C2EF07DD6A8841F6B46BDB60A53F378983	
Andrei RADU	andrei.radu(at)thalesgroup.com	0x99F98FD	Incident handler
	Fingerprint	1C0954E8D03415FC2959C11B4B95B83BB99F98FD	
Papa-Balla BABOU	papa-balla.babou(at)thalesgroup.com	0x32136137	Incident handler
	Fingerprint	B88DEECCCFEFFB1215C9E53FA9D4DDD132136137	

Belgium Core Team.

Name	Email	KeyID	Role
Dorian RETTER	dorian.retter(at)thalesgroup.com	0xC43BF8E4	Incident handler
	Fingerprint	B368290A6D2AEE7877454DE3B7E01D58C43BF8E4	

Senegal L1 Incident handling.

Name	Email	KeyID	Role
Ahmadou LO	alo(at)suricatesolutions.com	0x5D762D26	Incident handler
	Fingerprint	43B44A3650E18F62850290AF79B38E1C5D762D26	
Warkha NDAO	wndao(at)suricatesolutions.com	0x50662133	Incident handler
	Fingerprint	B9B5CAD8AAB47B0A25BAD40D8307C4D25066 2133	
Aboubakrine FALL	afall(at)suricatesolutions.com	0xE1A1F391	Incident handler
	Fingerprint	519C8A0D27D593B94CCA915470CE873FE1A1F391	
Cherif MAZID	cmazid(at)suricatesolutions.com	0xAA0294A3	Incident handler
	Fingerprint	E35E2F1F08AED336114E998BF0899C5CAA02 94A3	

Software and system support may be performed by the following team.

Name	**Email**	**KeyID**	**Role**
Benjamin FUHRO	benjamin.fuhro(at)thalesgroup.com	0x343131B7	Support
	Fingerprint	BC091234C3176DAF0A5FFD8237C6A6F6343131B7	
David VERNAZOBRES	david.vernazobres(at)thalesgroup.com	0x6F537549	Support
	Fingerprint	219625B534AFC1B0E036FC60C74D430F6F537549	
Quentin HOPP	quentin.hopp(at)thalesgroup.com	0x63004922	Support
	Fingerprint	01D19F2F0B8CBFC3DE9643975ECEAA8263004922	

Additional L1 Incident handling may be performed by the following team.

Name	**Email**	**KeyID**	**Role**
Sebastien KAISER	sebastien.kaiser(at)thalesgroup.com	0x5A81F9D3	Incident handler
	Fingerprint	0E6A08F80460CB59C7D294B19B1A1A805A81F9D3	
Renaud FRERE	renaud.frere(at)thalesgroup.com	0xD47B1777	Incident handler
	Fingerprint	EAA590EFF7B1653387724A8A173642E2D47B1777	

Business and legal support team members are:

Name	**Email**	**KeyID**	**Role**
Lionel THONNATTE	lionel.thonnatte(at)thalesgroup.com	0x8F049870	Business support
	Fingerprint	5DC9616B98E443FE738B903C31EDBF5B8F049870	

Other Information

General information about the TCS-CERT, as well as links to various recommended security resources, can be found at https://cds.thalesgroup.com/en/tcs-cert

Points of Customer Contact

The preferred method for contacting the TCS-CERT is via e-mail at <**team(at)tcs-cert.com**>; E-mails sent to this address will be automatically forwarded to the on-call person If you require urgent assistance, put "**[URGENT]**" in your subject line.

Emails could be encrypted using PGP. TCS-CERT public key information are detailed in the chapter

'Public keys and other encryption information'.

If it is not possible (or not advisable for security reasons) to use e-mail, TCS-CERT can be reached by telephone during regular office hours. (See chapter *Telephone number*) Outside these hours, incidents will be registered 24/7 through its SOC who may contact the Incident handler on duty. In this case, use the emergency number referenced in chapter *Telephone number*

If possible, when submitting your report, use the form mentioned in section *Incident Reporting Forms*.

Charter

Mission statement

TCS-CERT is a dedicated team part of Thales Cyber Solutions Luxembourg and Belgium and acts as the Computer Security Incident Response team (CSIRT) for Thales Cyber Solutions Luxembourg and Belgium formerly known as Excellium Group S.A.

TCS-CERT address mainly THALES Customers, it should not be confused with THA-CERT which is an internal Thales CERT. It is an operational team responsible for handling and managing IT security incidents that may impact Thales group.

The team's purpose is twofold: first, it implements proactive measures to reduce the risks of computer security incidents for their entity and its constituencies, but also any customer of Thales Cyber Solution. Secondly, TCS-CERT will aid them to adequately respond to such incidents.

TCS-CERT will address every kind of computer security incidents already ongoing or threatening to occur in the constituencies' networks. The incidents are first prioritized according to their apparent severity and extent. The level of support given by TCS-CERT might vary depending on the type of incident or issue, its severity and the CSIRT's available resources, but in any case, a response will always be provided. Additionally, TCS-CERT will release security notices based on relevancy of information.

To ensure its mission, TCS-CERT has been given mandate to warn application owners and users of known security issues and require fix to security configurations. Additionally, TCS-CERT will report directly relevant security issues related to Thales Cyber Solutions Luxembourg S.A. and constituencies to Thales Cyber Solutions Belgium S.A. CISO and managing partners.

This team establishment dates from January 2014, and a funding model has been put in place to ensure the long-term stability of this CSIRT.

TCS-CERT will occasionally work in cooperation with various CERTs and Security Operations Centers (SOC). TCS-CERT can also act as a CSIRT bridge to *Professionnels du Secteur Financier (PSF)* entities in Luxembourg to improve reaction and coordination in case of incidents.

Constituency

TCS-CERT is the Computer Security Incident Response Team of Thales Cyber Solutions Luxembourg S.A. and Thales Cyber Solutions Belgium S.A.

The constituency will cover various TLD, Internet Public ASN and IP addresses located/originated and/or operating in/from his customers.

Constituency type: Mixed

Constituency sector: Commercial

Sponsorship and/or affiliation

TCS-CERT is a private CSIRT. It is owned and operated by Thales Cyber Solutions.

It maintains relationships with various CSIRTs in Luxembourg and Belgium.

TCS-CERT is listed as team member of CERT.lu since 2015

https://www.cert.lu/#members

TCS-CERT is officially listed as certified team since 31 August 2023.

https://www.trusted-introducer.org/trusted-introducer/directory/teams/tcs-cert-lu

TCS-CERT is officially member of FIRST since 23 December 2019.

https://www.first.org/members/teams/tcs-cert

TCS-CERT is member of Cyber Security Coalition (Belgium) since 8 January 2021.

https://www.cybersecuritycoalition.be/members/

Policies

Types of Incidents and Level of Support

TCS-CERT addresses all types of computer security incidents which occur, or threaten to occur, in the constituency networks. The level of support given by TCS-CERT will vary depending on the type and severity of the incident or issue and CERT's available resources. However, in all cases, some responses will be made.

Incidents will be prioritized according to their apparent severity and extent.

Note that no direct support will be given to end users; they are expected to contact their system administrator, network administrator, or department head for assistance. The TCS-CERT will support the latter people.

Co-operation, Interaction and Disclosure of Information

TCS-CERT will exchange all necessary information with other CSIRTs as well as with affected parties' administrators.

TCS-CERT will protect sensitive information in accordance with relevant regulations and policies, regarding the rules requested by the CSSF (*Commission de Surveillance du Secteur Financier*) and the constraints of a support PSF entity.

TCS-CERT will append Light Traffic Protocol when sharing information with teams that support it and will honor such protocol if present.

For Vulnerabilities, TCS-CERT will follow its own responsible disclosure process. This process is available on demand.

Communication and Authentication

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

Unencrypted e-mail will not be considered particularly secure but will be sufficient for the transmission of low-sensitivity data.

If it is necessary to send highly sensitive data (i.e. information classified as Confidential) by e-mail, encryption (preferably PGP) will be used.

All e-mail or data communication originating from TCS-CERT will be digitally signed, using the generic PGP key mentioned above or the CERT team members own signature keys.

Services

Incident Response

TCS-CERT will assist system owners in handling the technical and organizational aspects of incidents. It will provide assistance and guidance with respect to the following aspects of incidents management.

Incident Triage

- Investigating whether an incident occurred.
- Determining the extent of the incident.

Incident Coordination

- Determining the initial cause of the incident.
- Facilitating contact with other sites which may be involved.
- Facilitating contact with the constituency and/or appropriate law enforcement officials, if necessary.
- Making reports to other CSIRTs.
- Composing announcements to users, if applicable .

Incident Resolution

Note: This set of service includes also incident response on-site.

- Technical analysis.
- Removing the vulnerability.
- Securing the system from the effects of the incident.
- Evaluating whether certain actions are likely to reap results in proportion to their cost and risk, in particular those actions aimed at an eventual prosecution or disciplinary action: collection of evidence after the fact, observation of an incident in progress, setting traps for intruders, etc.
- Collecting evidence where criminal prosecution, or University disciplinary action, is contemplated.

In addition, TCS-CERT will collect statistics concerning incidents and threats which occur within his customers and will notify the community as necessary to assist it in protecting against known attacks.

For requesting TCS-CERT services please refer to section *Incident Reporting Forms* and *Contact Information* for points of contact.

Please remember that amount of assistance will vary as described in section *Mission statement*.

Proactive Activities

Regarding its resources TCS-CERT will coordinate and maintain the following services:

- List of vulnerabilities.
- Threat notification.
- Training and educational services.

Incident Reporting Forms

TCS-CERT does not use any Incident Reporting Forms, we strongly encourage anyone reporting a security incident to use communication by email as described in chapter “Electronic Mail Address”.

Disclaimers

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

[End of document]

Copyright © 2025 – Thales Cyber Solutions. All rights reserved