



CERT - THUNT

RFC 2350

Prepared By: Thunt Labs Security
Date: April 2026
Reference: RFC2350-001

Historique des révisions

Version	Date	Auteur	Modifications
1.0	2026-04-16	Thunt Labs Security	Initial release

Contents

CERT-THUNT - RFC 2350	3
1. Summary	3
2. Document Information	3
2.1. Revisions	3
2.2. Distribution List for Notifications	3
2.3. Locations where the Document May Be Found	3
2.4. Authenticating this Document	3
2.5. Document Identification	3
3. Contact Information	3
3.1. Name of the Team	3
3.2. Address	3
3.3. Timezone	3
3.4. Telephone Number	3
3.5. Facsimile Number	3
3.6. Electronic Mail Address	3
3.7. Other Telecommunication	4
3.8. Public Keys and Encryption Information	4
3.9. Team Members	4
3.10. Other Information	4
3.11. Points of Contact	4
4. Charter	4
4.1. Mission Statement	4
4.2. Constituency	4
4.3. Sponsorship and/or Affiliation	4
4.4. Authority	4
5. Policies	4
5.1. Types of Incidents and Level of Support	4
5.2. Co-operation, Interaction and Disclosure of Information	5
5.3. Communication and Authentication	5
6. Services	5
7. Incident Reporting Forms	5
8. Disclaimers	5

CERT-THUNT - RFC 2350

1. Summary

This document describes the constituency, services, and operational policies of CERT-THUNT in accordance with RFC 2350.

2. Document Information

2.1. Revisions

Date	Version	Author	Comment
2026-04-16	1.0	THUNT LABS SECURITY	Initial published version based on ExdTrack template

2.2. Distribution List for Notifications

There is no distribution list for notifications.

2.3. Locations where the Document May Be Found

The current and latest version of this document is available at:

<https://www.thunt.eu/CERT-THUNT-RFC2350.md>

2.4. Authenticating this Document

This document is signed with the OpenPGP key of CERT-THUNT. The detached signature is published at:

· <https://www.thunt.eu/CERT-THUNT-RFC2350.md.sig>

2.5. Document Identification

- Title: CERT-THUNT - RFC 2350
- Version: 1.0
- Document Date: 2026-04-16
- Expiration: This document is valid until superseded by a later version.

3. Contact Information

3.1. Name of the Team

CERT-THUNT

3.2. Address

THUNT LABS SECURITY
42 BLD DE METZ
35700 RENNES
FRANCE

3.3. Timezone

CET/CEST

3.4. Telephone Number

Available on request.

3.5. Facsimile Number

Not available.

3.6. Electronic Mail Address

If you need to notify us about an information security incident or a cyber threat targeting or involving THUNT LABS SECURITY, please contact:

cert@thunt.eu

3.7. Other Telecommunication

Not available.

3.8. Public Keys and Encryption Information

CERT-THUNT uses an OpenPGP key dedicated to incident handling communications.

- Key ID: 0x77A5DCA9B34D8B99
- Fingerprint: 9221 5F37 867B B4E1 10D2 EDFD 77A5 DCA9 B34D 8B99
- Public key URL: <https://www.thunt.eu/.well-known/pgp-key.asc>

The public key shall be used whenever sensitive information must be sent to CERT-THUNT securely.

3.9. Team Members

CERT-THUNT is operated by THUNT LABS SECURITY personnel.

3.10. Other Information

General information about THUNT LABS SECURITY is available at:

<https://www.thunt.eu/>

3.11. Points of Contact

The preferred method to contact CERT-THUNT is by email:

cert@thunt.eu

Business hours are generally regular French business hours, Monday to Friday.

Emergency handling outside business hours may be provided on a best effort basis.

4. Charter

4.1. Mission Statement

CERT-THUNT is the security contact point for receiving, assessing, and coordinating the handling of security incidents affecting THUNT LABS SECURITY systems, services, users, and, where applicable, third-party assets covered by a contractual mandate or explicit authorization.

4.2. Constituency

The primary constituency of CERT-THUNT includes THUNT LABS SECURITY information systems, applications, infrastructure, services, and associated users.

The constituency may also include third-party systems, services, infrastructures, applications, and users where CERT-THUNT is designated to act under a contractual engagement, service agreement, incident response mandate, or other explicit authorization.

4.3. Sponsorship and/or Affiliation

CERT-THUNT is operated by THUNT LABS SECURITY.

4.4. Authority

CERT-THUNT acts on behalf of THUNT LABS SECURITY for incident intake, coordination, and security communications related to THUNT LABS SECURITY-operated assets.

For third-party assets, CERT-THUNT may act only within the scope expressly authorized by contract, mandate, or written approval from the relevant asset owner or responsible organization.

5. Policies

5.1. Types of Incidents and Level of Support

CERT-THUNT handles reports related to:

- compromise or suspected compromise of THUNT LABS SECURITY systems
- vulnerabilities affecting THUNT LABS SECURITY-operated services
- abuse or malicious activity originating from THUNT LABS SECURITY-operated assets
- phishing, fraud, or impersonation involving THUNT LABS SECURITY branding or infrastructure
- incidents affecting third-party assets where CERT-THUNT has an agreed response, coordination, investigation, or advisory role

Support is provided on a best effort basis.

5.2. Co-operation, Interaction and Disclosure of Information

CERT-THUNT will treat received information according to its sensitivity and operational need. Information may be shared with relevant internal stakeholders, affected parties, service providers, or authorities when necessary for incident handling, legal compliance, or protection of THUNT LABS SECURITY and third parties.

5.3. Communication and Authentication

Sensitive communications should use the published OpenPGP key of CERT-THUNT. This document and related public security material may be authenticated using detached OpenPGP signatures.

6. Services

CERT-THUNT provides:

- incident intake and triage
- coordination of incident response
- security communication for THUNT LABS SECURITY-operated assets
- initial analysis and routing of vulnerability disclosures
- incident response, coordination, and advisory support for third parties within the limits of agreed contractual or authorized scope

7. Incident Reporting Forms

Incidents should be reported by email to:

`cert@thunt.eu`

8. Disclaimers

While CERT-THUNT will make reasonable efforts to process and respond to incident reports, no guarantee is given regarding response time, completeness, or outcome.