TLP:WHITE

NaTran RFC 2350

1. Document Information

This document contains a description of NaTran-CERT in accordance with RFC 2350[1] specification. It provides basic information about Natran's Computer Security Incident Response Team, describes its roles and responsibilities.

1.1. Date of Last Update

This is the version 1.2 released on February 12th, 2025.

1.2. Distribution List for Notifications

There is no distribution list for notifications.

1.3. Locations where this Document May Be Found

The current and latest version of this document can be provided on demand by contacting cert@natrangroupe.com or on the NaTran's website at: www.natrangroupe.com/cert.

1.4. Authenticating this Document

This document has been signed with the PGP key of NaTran-CERT.
The PGP public key, ID and fingerprint are available on the NaTran's website at:
www.natrangroupe.com/cert

1.5. Document Identification

Title: NaTran-CERT RFC 2350
Version: 1.2
Document Date: 2025-02-12
Expiration: this document is valid until superseded by a later version

[1] https://tools.ietf.org/html/rfc2350

2. Contact Information

2.1. Name of the Team

Short name: NaTran-CERT
Full name: Computer Security Incident Response Team of NaTran

2.2. Address

CERT NaTran
15 avenue de l'Europe
92270 Bois Colombes
France

2.3. Time Zone

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

2.4. Telephone Number

None available

2.5. Facsimile Number

None available

2.6. Other Telecommunication

None available

2.7. Electronic Mail Address

cert@natrangroupe.com

2.8. Public Keys and Encryption Information

PGP is used for functional exchanges with cert@natrangroupe.com

- User ID : CERT NaTran <cert@natrangroupe.com>
- Key ID: 6F5B C8E1 F5B2 B90C
- Fingerprint: C3C3 B25C BD3D F8D1 501E 7991 6F5B C8E1 F5B2 B90C

The public PGP key is available at: www.natrangroupe.com/cert.

2.9. Team Members

NaTran-CERT is made up of cybersecurity experts in the fields of analysis, digital investigation, forensics and security incident response.

The list of team members is not publicly available..

2.10. Operating time

NaTran-CERT operates a 24/7/365 service for internal requests.

For external requests, it can be reached by email at the address given in section 2.7 Email. A reply will be given within working hours (between 8.00 am and 6.00 pm, Monday to Friday).

2.11. Points of Customer Contact

NaTran-CERT prefers to receive incident reports via e-mail given in section 2.7 Email.

Please use our PGP key to ensure integrity and confidentiality. See section Public Keys and Encryption Information.

In case of emergency, please specify the [URGENT] tag in the subject field in your e-mail. An answer will be given within working hours.

2.12. Other information

None

3. Charter

3.1. Mission Statement

The Operational Cybersecurity department of NaTran handles the operational aspects allowing the security posture of NaTran to be put into effect by maintaining and exploiting security and identity management tools, controlling the projects' cyber-compliance, supervising vulnerabilities, and handling cyber-incidents response.

The CERT of NaTran (NaTran-CERT) is the team responsible for incident-response, vulnerability analysis and remediation prioritization, and forensics. NaTran-CERT's mission is to anticipate and centralize the management of cyber threats to protect NaTran's IT. NaTran-CERT's activities cover prevention, detection and response.

The actions taken by NaTran-CERT are driven by several key values:

- NaTran-CERT strives to act according to the highest standards of ethics, integrity, honesty and professionalism,
- NaTran-CERT is committed to deliver a high-quality service to its constituency,
- NaTran-CERT will ensure to respond to security incidents as efficiently as possible,
- NaTran-CERT fosters information exchange with its peers on a need-to-know basis.

3.2. Constituency

NaTran benefits from all the services that NaTran-CERT can provide. See the "Services" section.

3.3. Sponsorship and/or Affiliation

The CEO of NaTran and the CISO of NaTran are the main sponsors of NaTran-CERT.

3.4. Authority

NaTran-CERT operates under the authority of the NaTran Chief Information Security Officer.

4. Policies

4.1. Types of Incidents and Level of Support

NaTran-CERT is authorized to handle all types of cyberattacks that could hamper the confidentiality, integrity, or availability of NaTran's systems and processes.

Depending on the security incidents' type, NaTran-CERT will gradually roll out its services which include cybersecurity incident response and digital forensics. The level of support given by NaTran-CERT will vary depending on the severity of the security incident or issue, its potential or assessed impact and the available NaTran-CERT's resources at the time.

4.2. Co-operation, Interaction and Disclosure of Information

NaTran-CERT highly considers the paramount importance of operational coordination and information sharing between CSIRT, CERT, SOC and similar actors, and also with other organizations, which may aid to deliver its services or which provide benefits to NaTran-CERT.

NaTran-CERT operates within the current French legal framework.

4.3. Communication and Authentication

NaTran-CERT protects sensitive information in accordance with relevant French and European regulations and policies within France and the EU.

In particular, NaTran-CERT respects the sensitivity markings defined by originators of information.

NaTran-CERT also recognizes and supports the FIRST TLP (Traffic Light Protocol) version 2.0.

Communication security (which includes both encryption and authentication) is achieved using PGP primarily or any other agreed means, depending on the sensitivity level and context.

5. Services

This section describes NaTran' CERT services.

5.1. Incident response

5.1.1. Incident Triage

NaTran-CERT receives, analyzes and prioritizes all cybersecurity-related incidents to enable effective handling and remediation.

5.1.2. Incident Detection

NaTran-CERT maintains, operates and enhances detection tools and services to ensure optimal intrusion detection.

5.1.3. Incident Coordination

NaTran-CERT handles the coordination of actors within NaTran and with external parties to ensure swift remediation.

5.1.4. Incident Resolution

NaTran-CERT provides forensics on compromised systems and advises all parties on the best way to mitigate then eliminate the threat.

5.2. Proactive activities

5.2.1. Vulnerability Analysis

NaTran-CERT receives, analyzes and prioritizes software vulnerabilities affecting our IT systems to enable quick and effective remediation.

5.2.2. Penetration testing

NaTran-CERT performs internal penetration testing on NaTran infrastructure.

6. Incident Reporting Forms

To report an external incident from the outside, please provide NaTran-CERT the following details :

- Summary of the event: incident/alert/crisis,
- contact details such as person or organization’s name, address, email address, phone number,
- PGP key if available,
- IP address(es), email, FQDN(s), file hash, and any other relevant technical element.

Please note that in case you desire to forward any email message to NaTran-CERT, please include all relevant email headers, bodies and any attachments if possible and as allowed by the regulations, policies and legislation under which you operate.

7. Disclaimers

While every precaution will be taken in the preparation of information, notifications, and alerts, NaTran-CERT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.