TLP:WHITE

CERT ENEDIS

RFC 2350

Identification : CERT-Enedis_RFC2350
Version : 1.0

Summary
This document is the RFC 2350 for CERT ENEDIS Team. It describes contacts, roles and responsibilities linked to CERT ENEDIS.

Version History

Version	Date	Nature de la modification	version replaced
1.0	07/05/2020	Document creation	N/A

Diffusion

☑ Libre ☐ Interne ☐ Restreinte ☐ Confidentielle

ENEDIS
L'ELECTRICITE EN RESEAU

TLP:WHITE

TLP:WHITE

1. Document information

This document contains a description of CERT ENEDIS (CERT-Enedis) as implemented by RFC 2350. It provides basic information about CERT-Enedis, its communication channels, its roles and responsibilities.

1.1. Date of last update

Version 1.0, Published on 2020-05-07

1.2. Distribution list for notifications

Notification of document changes is not distributed by a Mailing List or any other mechanisms.

1.3. Location where this Document May be Found

The latest document version of this document is available on ENEDIS Website located at **https://www.enedis.fr/contenu-html/cert/index.html**

1.4. Authenticating this Document

This document has been signed with the PGP Key of CERT-Enedis. The public key is available at **https://www.enedis.fr/contenu-html/cert/index.html**

1.5. Document Identification

- Title: CERT-Enedis_RFC2350
- Version: 1.0
- Date: 2020-05-07
- Expiration: this document is valid until superseded by a later version

2. Contact information

2.1. Name of the CSIRT Team

- Official Name: **CERT ENEDIS**
- Short Name: **CERT-Enedis**

2.2. Address

Below the full postal address of the CERT Team:

CERT-ENEDIS
ENEDIS
117 Boulevard Vivier Merle
69003 LYON, FRANCE

2.3. Time Zone

The time zone associated to the CERT-ENEDIS operations is: **CET/CEST**

2.4. Telephone Number

A public telephone number is available for emergency calls (24/7): **+33 806 800 300**

2.5. Mailing Address

To report any cybersecurity incident or a cyber-threat targeting, please contact us at the following address: **cert@enedis.fr**

2.6. Facsimile Number

N/A

2.7. Public Keys and Encryption Information

PGP is used for secure dialog with CERT-Enedis.

- Key ID: 6B1A 5284
- Fingerprint: F7F5 C046 7739 2DF4 4DAC E9C2 6B1A 5284 5533 7A7D

The public PGP key is available at: **https://www.enedis.fr/contenu-html/cert/CERT%20Enedis.asc**

2.8. Team Members

The full list is not publicly available. According to his role the team is made of Cybersecurity engineer and Cybersecurity analysts. The CERT-Enedis team leader is Christian MARTINEZ.

2.9. Points of customers contact

The preferred method to contact the CERT-Enedis is by sending an email using the following address: **cert@enedis.fr**
Please use our cryptographic key to ensure integrity and confidentiality.
In case of emergency, please specify the [URGENT] tag in the subject field in your e-mail. An analyst will be assigned during working hours.

If necessary an emergency call number is available 24/7: +33 806 800 300

3. Charter

3.1. Mission Statement

The CERT-Enedis team's activities are non-profit and fully financed by ENEDIS S.A.

CERT-Enedis is part of the ENEDIS Cybersecurity Pole within Enedis management information systems. CERT-Enedis is the team in charge of incident detection, incident response, digital forensics, malware analysis, and threat intelligence activities for ENEDIS.

The mandate of the CERT-Enedis is:

- **Anticipate** threats and malicious behavior that can occurs against ENEDIS activities. This is achieved using tools and knowledge related to cyber threat intelligence and OSINT;
- **Detect** threats and malicious behavior that can occurs against ENEDIS. This is achieved in cooperation with other teams in order to deliver Cybersecurity expertise to detect malicious activities and/or behavior inside and/or targeting ENEDIS Information systems;
- **React** as best as possible against a cyberattack in progress inside and/or targeting ENEDIS Information systems. The CERT-Enedis has the mission to coordinate the Cyber crisis management and use all technics and tactics at his disposal to stem the cyberattack occurring (in accordance with the Enedis Top management);
- **Coordinate** the remediation phase with all other teams/partners in order to secure the damaged IT systems.

3.2. Constituency

The constituency of CERT-Enedis is composed of all the elements of ENEDIS Information System: its users, its systems, its applications and its networks.

3.3. Affiliation

CERT-Enedis is affiliated to ENEDIS. It maintains contact with various nationals and internationals CERT entities.

3.4. Authority

The CERT Team is responsible to anticipate, detect, react and coordinate the remediation across the whole company for all perimeters (corporate and industrial IT systems). CERT-ENEDIS operates under the authority of the ENEDIS Chief Information Security Officer.

4. Policies

4.1. Types of Incidents and Level of Support

CERT-Enedis handles all type of incidents related to cyberattacks and/or Cyber threats for ENEDIS. The level of support associated to them could be different and change regarding the nature, the target or the complexity. The level of support can change until involve digital forensics and coordinate the incident response.

The services provided by CERT-Enedis includes:

- Vulnerability and threat intelligence analysis;
- Vulnerability response and coordination;
- Cybersecurity Incident detection;
- Cybersecurity Incident analysis and forensics;
- Cybersecurity Incident response and remediation coordination.

CERT-Enedis operates under the current French legal framework.

4.2. Cooperation, Interaction and Disclosure of Information

CERT-Enedis knows the importance for sharing information with third parties. The "need to know" principle is applied in order to share the necessary amount of information to the restricted people/organizations involved. In addition CERT-Enedis respects the Information Sharing Traffic Light Protocol (TLP) that comes with the tags WHITE, GREEN, AMBER or RED as described by the FIRST definitions at: www.first.org/tlp/

CERT-Enedis can exchange with other entities such as external SOC, CERT and other Cybersecurity teams in order to facilitate information sharing. CERT-Enedis dialogs and cooperates with a privilege way with Cybersecurity entities close to their activities.

4.3. Communication and Authentication

The preferred way to exchange information and communicate with CERT-Enedis is via email.

CERT-Enedis recommend to use cryptographic PGP to communicate securely with them. The TLP tag is also recommended in order to facilitate the initial triage realized by the team.

5. Services

The CERT-Enedis services is provided during working hours. For emergency, a call number is available 24/7.

5.1. Incident Response

5.1.1. Incident Triage

The incident triage is divided in several parts to contextualize, categorize and define a severity level associated to the incoming incident.

- **Categorization**: the security incident is associated to a category depending on their nature. (CERT-Enedis uses ETSI ISI as Categorization format);
- **Contextualization**: based on internal and/or external information additional information are added to the incident for enrichment;
- **Severity level**: A severity is applied depending on multiple factors and divided in three levels: Low, Medium, High.

5.1.2. Incident coordination

In regards to the Incident triage the coordination could be done in different ways:

- Notifications : can be sent to the involved parties for information/remediation;
- Blocking actions: can be asked to a third party based on the attack categorization.

5.1.3. Incident Resolution

In regards to the Incident categorization and severity level the resolution could involve:

- The analysis of compromised systems;
- Digital forensics;
- Disaster recovery plan to be performed.

5.1.4. Proactive activities

The proactive activities is done by a "purple team" inside CERT-Enedis team. These activities are:

- Threat intelligence monitoring;
- Vulnerability exposure monitoring;
- IOC sharing.

5.2. Incident Reporting Forms

CERT-Enedis uses specific forms templates for its own usage and restricted to ENEDIS.

To report security incident from outside involving ENEDIS, please provide the following details

Type	Information
Organization name	
Contact details	
Issue description	
Technical details	

6. Disclaimers

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