ENGIE CERT

RFC 2350

Version : 1.4

Date : 09/02/2023

Table of Contents

1 Document Information

This document contains a description of ENGIE CERT according to RFC 2350.

It provides information about the CERT, how to contact the team, and describes its responsibilities and the services offered by ENGIE CERT.

1.1 Document Identification

Title: 'ENGIE CERT RFC 2350'
Version: 1.4
Document Date: 09-02-2023

1.2 Date of Last Update

Version 1.3, published on 17-02-2022

1.3 Distribution List for Notifications

There is no distribution list for notifications.

1.4 Location & Authenticity

The current version of this document as well as the signature of the document are available on ENGIE CERT's website: https://www.engie.com/CERT

2 Contact Information

2.1 Name of the Team

ENGIE CERT

2.2 Address

ENGIE CERT
1 place Samuel Champlain
92930 Paris La Defense
FRANCE

2.3 Time Zone

CET/CEST (UTC +1/UTC +2)
Central European Time / Central European Summer Time

2.4 Telephone Number

+33 1 49 18 24 28.

2.5 Facsimile Number

None.

2.6 Other Telecommunication

None.

2.7 Electronic Mail Address

Shall you need to notify us about a cyberthreat or an information security incident targeting or involving ENGIE or any of its subsidiaries, please contact us at:

cert@engie.com

2.8 Public Keys and Other Encryption Information

To send us information securely, please use our PGP key:

- Key ID: 0x543D463A6B412284
- Fingerprint: 01D7 E06D 6864 8093 DADA F7E7 543D 463A 6B41 2284
- The public PGP key is available at https://www.engie.com/sites/default/files/assets/documents/2023-02/ENGIE%20CERT_0x6B412284_public.asc

2.9 Team Members

The team leader is Omar ABDELMOUMEN. The team consists of IT security professionals.

2.10 Other Information

The ENGIE CERT webpage is available at: https://www.engie.com/CERT

2.11 Points of Customer Contact

ENGIE CERT prefers to receive incident reports via e-mail. Please use our cryptographic keys above to ensure integrity and confidentiality.
ENGIE CERT's hours of operation are restricted to regular business hours (09:00-18:00 Monday to Friday), all year long.

3 Charter

3.1 Mission Statement

ENGIE CERT is responsible for providing alerts and warnings, intrusion detection services, incident handling, artifact handling and development of security tools for ENGIE Group companies and subsidiaries.

3.2 Constituency

Our constituency are composed of ENGIE Group and all subsidiaries.
For a complete list and more information please see https://www.engie.com

3.3 Sponsorship and/or Affiliation

ENGIE CERT is the Computer Security Incident Response Team (CSIRT) for the ENGIE Group.

3.4 Authority

We coordinate security incidents involving our constituency.
ENGIE CERT operates under the auspices of, and with authority delegated by, the ENGIE Group Digital & IT Department (Direction du Digital & des Systèmes d'Information), ENGIE S.A.

4 Policies

4.1 Types of Incidents and Level of Support

ENGIE CERT addresses all kinds of security incidents which occur, or threaten to occur, within its constituency.
The level of support depends on the type and severity of the given security incident, the amount of affected entities within our constituency, and our resources at the time.
The level of support given by ENGIE CERT depends on the severity of the security incident, its impact and the availabilities of ENGIE CERT's resources at the time.
ENGIE CERT will act on information it receives about vulnerabilities which create opportunities for future incidents.

4.2 Co-operation, Interaction and Disclosure of Information

ENGIE CERT will exchange all necessary information with other CSIRTs as well as with other affected parties if they are involved in the incident or incident response process.

No incident or vulnerability related information will be given to other persons. French law enforcement personnel requesting information in the course of a criminal investigation will be given the requested information within the limits of the court order and the criminal investigation, if they present a valid court order from a French court.

4.3 Communication and Authentication

All e-mails sent to the ENGIE CERT should be signed using PGP. All e-mails containing confidential information should be encrypted and signed using PGP.
Information received in encrypted form should not be stored permanently in unencrypted form.

For other communication, a phone call, postal service, or unencrypted e-mail may be used. ENGIE CERT supports the Information Sharing Traffic Light Protocol (ISTLP).

5 Services

5.1 Reactive Activities

The team offers the following reactive services:

- Alerts and Warnings
- Incident Handling
- Artifact Handling
- Vulnerability Response Coordination

5.2 Proactive Activities

The team offers the following services:

- Intrusion detection services
- Information services
- Auditing services

6 Incident Reporting Forms

No incident reporting form has been developed to report incidents to ENGIE CERT. Please report security incidents via encrypted e-mail to cert@engie.com with at least the following information:

- Contact details and organizational information;
- Date, time & time zone of the incident (indicate if provided info is an assumption);
- IP address(es), FQDN(s), and any other relevant technical element with associated observation;
- The impact of the incident (in terms of confidentiality, integrity & availability);
- Indicate if PII might be impacted (data leak, unauthorized access, …);
- Any relevant information about a threat or an incident related to ENGIE CERT constituency;
- The information sharing traffic light protocol.

7 Disclaimers

While all precautions are taken in the preparation of information, notifications and alerts, ENGIE CERT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information it provides.