BRIGHTWAY
Bring your business to the right way

BrightwayCERT

BRIGHTWAYCERT

« RFC-2350 – Description of services »

C0 – Public Usage

Ref. DO-BR-RFC2350-01
Date : 12/03/2022

Table of Contents

1. Preamble

1.1 About this document

This document contains a description of BrightwayCERT in accordance with RFC 2350. It provides basic information about BrightwayCERT, its channels of communication, and its roles and responsibilities.

1.2 Date of release/last update

Version 1.0 – 12 March 2022

1.3 Document availability

The current version of this document can be found at : https://brightway.fr/en/expertises/monitoring-response/
It can also be received by email by sending a request to : contact@brightway.fr.

1.4 Document identification and authentication

Title : BrightwayCERT_RFC2350
Version : 1.0
Release/Update Date : 2022-03-12
Expiration : this document is valid until superseded by a later version

2. Contact Information

2.1 Name of the team

Full name: BrightwayCERT
Short name: BrightwayCERT

2.2 Address

Brightway, 16 Rue Troyon, 92310 Sèvres

2.3 Email

For any urgent request or incident report, please write to us at incident@brightway.fr using BrightwayCERT PGP key.

2.4 Time Zone

CET/CEST: Paris (UTC+01:00, and UTC+02:00 summertime)

2.5 Telephone number

+33 1 45 34 35 38 – Available during office hours.

2.6 Facsimile number

N/A

2.7 Internet Website

https://www.brightway.fr

2.8 Public keys and encryption

BrightwayCERT uses the following PGP Key for functional exchanges with its constituency:

- **User ID:**
- **Key ID:**
- **Fingerprint:**

The public PGP key is available at the following location: https://brightway.fr/en/site-security/

2.9 Team members

BrightwayCERT team leader is Sami Chamam.
The team is composed of IT security experts (Incident Response Specialists, Threat Intelligence Analysts, Vulnerability Management Experts, Forensics Investigators, Security Awareness Trainers, etc.).
The nominative list of team members is not publicly available. Nevertheless, their identities might be divulged on a case-by-case basis according to the need-to-know restrictions.

2.10 Operating hours

The working hours of BrightwayCERT are from Monday to Friday, 09:00 to 18:00 Paris Time. Average response time is around 24 hours.

3. Charter

3.1 Mission statement

BrightwayCERT is Brightway's company dedicated Computer Emergency Response Team (CERT). Its main mission is to provide support to both public and private sector organizations with their efforts to investigate and respond to IT security incidents.
BrightwayCERT missions' include prevention, detection, response and recovery via:

- Helping its constituents prevent security incidents by setting up necessary protection measures (vulnerabilities management, CTI, Assets hardening, Awareness training, …);
- Sharing information on cyber threats with its constituents and partners;
- Conducting incident response activities;
- Participating in trusted networks of CSIRTs and CERTs such as FISRT

3.2 Constituency

BrightwayCERT constituents are located across all Metropolitan France territories and encompass a variety of private sector organizations such as banking institutions, industrial companies, insurance providers, manufacturing firms, and information technology businesses.
Secondary constituents are all public sector organisations such as government agencies, critical infrastructure providers, and non-profit organizations.

3.3 Affiliation / Sponsoring organization

BrightwayCERT is a private industrial CERT, owned, operated, and financed by Brightway SAS.

3.4 Authority

BrightwayCERT is placed under the authority of the SOC Manager.
BrightwayCERT works internally in cooperation with other Brightway departments (GRC, Pentesting, R&D, …).
BrightwayCERT cooperates externally with other national and international CERTs and CSIRTs.

4. Policies

4.1 Types of incidents and level of support

BrightwayCERT will process any security incident related to its mission.
BrightwayCERT level of support will be adjusted to provide adapted level of answer on any threat, vulnerability, incident analysis (assessment, impact, remediation).
The level of support given by BrightwayCERT will vary depending on the type and severity of the incident or issue, the type of constituent, the importance of the impact on critical or essential infrastructure or service, and BrightwayCERT available resources at the time.

4.2 Co-operation, interaction, and disclosure of information

By default, information is categorized as **confidential and cannot be shared outside the team** (BrightwayCERT and Client) without the authorization of Brightway SOC manager and the client CISO.
A specific level of confidentiality may be assigned to the security-related information, on a case-by-case basis and subject to the applicable procedure by the client.

4.3 Communication and authentication

The preferred method of communication is email. To contact BrightwayCERT, please send an email to: incident@brightway.fr (for sensitive communication) or contact@brightway.fr (for non-sensitive communication).

For the exchange of sensitive information and authenticated communication, the following PGP key can be used:

- **Name:**
- **ID:**
- **Fingerprint:**

Key is available on following platforms:

- https://brightway.fr

5. Services

BrightwayCERT's services include reactive and proactive services:

- 8/5 on-call duty;
- alerts and warnings;
- incident analysis and forensics;
- incident response assistance and support;
- incident response and remediation (also on-site);
- vulnerability and malware analysis;
- vulnerability response;
- threat intelligence analysis and sharing;
- Security Awarness and Training.

6. Incident Reporting Forms

To report an incident to BrightwayCERT, please provide following information:

1. Contact details (name/email and optionally phone number).
2. Date of Incident discovery
3. Incident general description

4. Affected asset(s).
5. Technical information subject to technical and legal feasibility.

Incident reporting form is sent by email to incident@brightway.fr .
Sensitive information must be encrypted using BrightwayCERT PGP Key.

7. Disclaimer

While BrightwayCERT will take every precaution in the preparation of information, notifications and alerts, and it will apply its best competence and effort in the performance of its services; Brightway SAS. assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.

All intellectual property rights in any reports, document, graphs, charts, photographs or any other material (in whatever medium) produced by BrightwayCERT in the performance of its services, including all rights in concepts, ideas and inventions that may arise, shall belong to Brightway SAS.