CERT Banque de France

CERT-BDF RFC 2350

TLP:WHITE

Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.

TLP: WHITE information may be distributed without restriction, subject to copyright controls.

Contents

1 Document Information

This document contains a description of CERT Banque de France (CERT-BDF) as implemented by RFC 2350[1]. It provides basic information about CERT-BDF, its channels of communication, its roles and responsibilities.

1.1 Date of Last Update

Version 4, updated on 2017-01-21.

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 is available from CERT-BDF's website. Its URL is:

https://cert.banque-france.fr/static/CERT-BDF-RFC2350-EN.pdf

1.4 Authenticating this Document

This document has been signed with the PGP key of CERT-BDF. The signature is available from CERT-BDF's website. Its URL is:

https://cert.banque-france.fr/static/CERT-BDF-RFC2350-EN.pdf.sig

1.5 Document Identification

Title: 'CERT-BDF RFC 2350'
Version: 4
Document Date: 2017-01-21
Expiration: this document is valid until superseded by a later version

2 Contact Information

2.1 Name of the Team

CERT-BDF: CERT Banque de France

2.2 Address

CERT-BDF
013-2146
31 rue Croix des Petits-Champs
75049 PARIS cedex 01
FRANCE

2.3 Time Zone

CET/CEST

[1] http://www.ietf.org/rfc/rfc2350.txt

2.4 Telephone Number

+33 1 42 92 93 02 (French business hours).

2.5 Facsimile Number

None available.

2.6 Electronic Mail Address

If you need to notify us about an information security incident or a cyber-threat targeting or involving Banque de France, please contact us at:

cert@banque-france.fr

2.7 Other Telecommunication

None.

2.8 Public Keys and Encryption Information

CERT-BDF has a PGP key:

- ID: 0xED92F9C3
- Fingerprint: 80E0 9E1F 7ACE C265 CD82 6638 C2E6 A117 ED92 F9C3

The key can be retrieved from one of the usual public key servers such as http://pgp.mit.edu/.

The key shall be used whenever information must be sent to CERT-BDF in a secure manner.

2.9 Team Members

CERT-BDF's team leader is Saâd Kadhi. The team consists of IT security analysts.

2.10 Other Information

General information about CERT-BDF can be found at the following URL:

https://cert.banque-france.fr/

2.11 Points of Customer Contact

The preferred method to contact CERT Banque de France is to send an email to the following address:

cert@banque-france.fr

A duty security analyst can be contacted at this email address during hours of operation.

If necessary, urgent cases can be reported by phone (+33 1 42 92 93 02) during French business hours.

CERT-BDF's hours of operation are usually restricted to regular French business hours (Monday to Friday 09:30 to 18:00).

3 Charter

3.1 Mission Statement

Within Banque de France, the 'Security Operations Center' (COS for Centre Opérationnel de Sécurité) department translates the security strategy in an actionable plan, controls the security level, responds to cyberattacks and establishes the operational security rules.

CERT Banque de France (CERT-BDF) is the COS unit in charge of security controls, digital forensics and incident response (DFIR) activities.

CERT-BDF's mission is to support Banque de France, the French national central bank, and to protect it from intentional and malicious attacks that would hamper the integrity of its IT assets or harm its interests. CERT-BDF's activities cover prevention, detection, response and recovery.

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

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

3.2 Constituency

CERT-BDF's constituency is composed of all the elements of Banque de France's Information System: its users, its systems, its applications and its networks.

3.3 Affiliation

CERT-BDF is affiliated to Banque de France. It maintains contacts with various national and international CSIRT and CERT teams according to its needs and the information exchange culture that it values.

3.4 Authority

CERT-BDF operates under the authority of the Deputy Secretary General in charge of Banque de France's Organization and Information Systems.

4 Policies

4.1 Types of Incidents and Level of Support

CERT-BDF is authorized to handle all types of cyberattacks that would hamper the integrity of Banque de France's IT assets or harm its interests.

Depending on the security incident's type, CERT-BDF will gradually roll out its services which include incident response and digital forensics.

The level of support given by CERT-BDF will vary depending on the severity of the security incident or issue, its potential or assessed impact and the available CERT-BDF's resources at the time.

4.2 Co-operation, Interaction and Disclosure of Information

CERT-BDF highly considers the paramount importance of operational coordination and information sharing between CERTs, CSIRTs, SOCs and similar bodies, and also with other organizations, which may aid to deliver its services or which provide benefits to CERT-BDF.

CERT-BDF operates within the current French legal framework.

CERT-BDF also complies with the CCoP (CSIRT Code of Practice) version 2.1[2].

4.3 Communication and Authentication

CERT-BDF protects sensitive information in accordance with relevant French and European regulations and policies within France and the EU. In particular, CERT-BDF respects the sensitivity markings allocated by originators of information communicated to CERT-BDF ("originator control").

CERT-BDF also recognizes and supports the ISTLP (Information Sharing Traffic Light Protocol) version 1.1[3].

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

5.1 Announcements

CERT-BDF provides information on the threat landscape, published vulnerabilities, new attack tools or artifacts and security measures needed to protect its constituency's Information System.

5.2 Alerts and Warnings

CERT-BDF disseminates information on cyberattacks, disruptions, security vulnerabilities, intrusion alerts, malware, and provides recommendations to tackle the issue within its constituency. Alerts and warnings may be passed on to other CERTs, CSIRTs, SOCs and similar bodies if deemed necessary or useful to them on a need-to-know basis.

[2] https://www.trusted-introducer.org/CCoPv21.pdf
[3] https://www.trusted-introducer.org/ISTLPv11.pdf

5.3 Pre-emptive Security Controls

CERT-BDF performs pre-emptive security controls to detect potential breaches or vulnerabilities and misconfigurations that may be leveraged in cyberattacks. The security controls also check the compliance level of various systems and applications with the security policies.

5.4 Development of Security Tools

CERT-BDF develops security tools for its own use, to improve its services and support its activities as needed. These security tools can be used by other members of its constituency or by members of the larger CERT, CSIRT and SOC communities in which CERT-BDF is one of the participants.

5.5 Intrusion Detection

CERT-BDF leverages a number of systems and processes to detect potential intrusions.

5.6 Digital Forensics and Incident Response

CERT-BDF performs incident response for its constituency. The incident response service as developed by CERT-BDF covers all '6 steps': preparation, identification, containment, eradication, recovery and lessons to be learned.

CERT-BDF also performs digital forensics whenever necessary including hard drive and memory forensics.

6 Incident Reporting Forms

No local form has been developed to report incidents to CERT-BDF.

In case of emergency or crisis, please provide CERT-BDF at least the following information:

- contact details and organizational information – name of person and organization name and address,
- email address, telephone number;
- IP address(es), FQDN(s), and any other relevant technical element with associated observation;
- scanning results (if any) - an extract from the log showing the problem;
- in case you wish to forward any emails to CERT-BDF, please include all email headers, body and any attachments if possible and as permitted 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, CERT-BDF assumes no responsibility for errors or omissions, or for damages resulting from the use of the information it provides.