1. Document Information

This document contains a description of the CERT-BSPP in accordance with RFC 2350[1] specification. It provides basic information about the CERT-BSPP, describes its responsibilities and services offered.

1.1. Date of Last Update

Version 1.0, published on 2022-10-4.

1.2. Distribution List for Notifications

Changes to this document are notified by email to:

- InterCERT France / network of French CSIRTs - intercert-france.fr

Please send questions about updates to CERT-BSPP team email address: cert@pompiersparis.fr

1.3. Locations where this Document May Be Found

cert.pompiersparis.fr

1.4. Authenticating this Document

This document has been signed with the PGP key of CERT-BSPP.
The PGP public key, ID and fingerprint are available on the CERT-BSPP's website at: cert.pompiersparis.fr/pgp_key.asc

1.5. Document Identification

Title: 'CERT-BSPP_RFC2350_EN'
Version: 1.0
Document Date: 2022-10-4

2. Contact Information

2.1. Name of the Team

Official name:
CERT-BSPP, Section sécurité des Systèmes d'informations de la Brigade de Sapeurs-pompiers de Paris (BSPP), the Paris Fire departement computer emergency response team.
Short name: CERT-BSPP

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

2.2. Address

Brigade de Sapeurs-pompiers de Paris
Etat-Major BSPP - Equipe CERT
1 Place Jules Renard
75017 Paris, FRANCE

2.3. Time Zone

CET/CEST

2.4. Telephone Number

Main number (duty office): + 33 (0)1 75 62 41 58 - **This number is not emergency rescue line.**
In case of emergency, dial number 18 or 112.

2.5. Other Telecommunication

Not applicable

2.6. Electronic Mail Address

If you need to notify us about an information security incident or a cyber-threat targeting or involving CERT-BSPP, please contact us at: cert@pompiersparis.fr

2.7. Public Keys and Encryption Information

PGP is used for functional exchanges with CERT-BSPP.

- User ID: CERT-BSPP <cert[at]pompiersparis.fr
- Key ID: 0x1B374948
- Fingerprint: 0176 06FD 0ACA 3401 1183 C19C 0570 5050 1B37 4948

The public PGP key is available at: cert.pompiersparis.fr/pgp_key.asc It can be retrieved from one of the usual public key servers.

2.8. Team Members

The list of the CERT-BSPP's team members is not publicly available. The identity of CERT-BSPP's team members might be divulged on a case by case basis according to the need to know restrictions.

2.9. Points of Customer Contact

CERT-BSPP prefers to receive incident reports via e-mail at cert@pompiersparis.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.

CERT-BSPP ‘s hours of operation are 7/7 24h all year long.

3. Charter

3.1. Mission Statement

CERT-BSPP is the Computer Emergency Response Team of the Paris fire department cyber security authority. Its mission is to coordinate and investigate IT security incident response for the Brigade de Sapeurs-Pompiers de Paris as a critical national infrastructure operators and operators of essential services as defined by the French law.

CERT-BSPP missions cover prevention, detection, response and recovery by:

- Helping to prevent security incidents in set up necessary protection measures;
- Detecting vulnerabilities on networks and systems;
- Managing incident response, with the support of trusted partners if necessary.

3.2. Constituency

The primary constituency is the Brigade de Sapeurs-Pomiers de Paris’s Military Bases located in the City of Paris and the surrounding départements of Seine-Saint-Denis, Val-de-Marne, and Hauts-de-Seine It also serves the Centre Spatial Guyanais in Kourou and the DGA Military Rocket Test Centre in Biscarosse.

3.3. Affiliation

CERT-BSPP is part of the Section Sécurité des Systèmes d’informations (Section SSI) of the Brigade de Sapeurs-pompiers de Paris, the Paris Fire departement computer security team.

3.4. Authority

French Ministry of the interior
Police Prefecture/Brigade de Sapeurs-pompiers de Paris

4. Policies

4.1. Types of Incidents and Level of Support

CERT-BSPP is the central point of contact regarding security-related computer incidents within the BSPP. The level of support given by the CERT-BSPP will vary depending on the type and severity of the

incident or issue, the type of constituent and the importance of the impact on critical or essential infrastructure or services.
CERT-BSPP's services include reactive and proactive services:

- 24-hour on-call duty;
- Alerts and warnings;
- Incident analysis and forensics;
- Incident response assistance and support;
- Incident response and remediation;
- Vulnerability and malware analysis;
- Vulnerability response;
- Threat intelligence analysis and sharing.

In addition, CERT-BSPP liaises and is able to request to a matrix of other expertise and knowledge provided by other French government and/or military offices.

4.2. Co-operation, Interaction and Disclosure of Information

General incident related information such as names and technical details is not published without agreement of the named parties. If not agreed otherwise, supplied information is kept confidential. CERT-BSPP will never pass information to third-parties unless required by law. Under the condition of acceptance through affected parties or authorized by law, CERT-BSPP prefers to share Tactics, Techniques and Procedures for the purpose of prevention and reaction to specific incidents.

Therefore such information might be passed to entities such as:

- French military and/or ministry of the interior own technical experts;
- Affected parties in our constituency;
- Affected ISPs/hosting providers in France;
- French law enforcement agencies (if required by law or on request from information source);
- CERT/CSIRT cooperation groups as named in Section 1.2;

All information is passed depending on its classification and the need-to-know principle. Only the specifically relevant and anonymised extracts are passed on. CERT-BSPP respects the Information Sharing Traffic Light Protocol (TLP) that comes with the tags as described by the FIRST definitions at: www.first.org/tlp/

CERT-BSPP handles and processes information in secured physical and technical environments in accordance with the French state regulations for the protection of information.

4.3. Communication and Authentication

The preferred method of communication is email. For the exchange of sensitive information and authenticated communication CERT-BSPP uses several encryption solutions. By default, all sensitive communication to CERT-BSPP should be encrypted with our public PGP key detailed in Section 2.7.

5. Services

5.1. Incident response

CERT-BSPP's incident response services are available on a 24/7 basis to our constituency. All information and communication technologies related incidents are evaluated. In-depth analysis is provided by technical experts.

5.2. Incident Triage

- Assessment of the severity of the incident by the duty officer
- If required, escalation to the general management.

5.3. Incident Coordination

- Categorization of the incident related information with respect to the information disclosure policy.
- Notification of other involved parties on a need-to-know basis, as per the information disclosure policy.

5.4. Incident Resolution

- This may include analysis of compromised systems.
- Elimination of the cause of a security incident (the vulnerability exploited) and its effects (for example, continuing access to the system by an intruder).

5.5. Proactive activities

- Network monitoring to detect attacks as early as possible.
- Training security officers.
- Risk analysis
- User sensibilisation

6. Incident Reporting Forms

The reporting of security incidents involving the government, critical national infrastructure operators, operators of essential services and digital service providers is based on specific secured reporting forms and procedures. No specific form is needed to report security incidents from other parties.

7. Disclaimers

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