RFC 2350

1 DOCUMENT INFORMATION

This document contains a description of computer security incident response team of judicial police (CSIRT-PJ) depending on French National Police / Central Directorate of Judicial Police / Cybercrime Sub-directorate, as implemented by RFC 2350. It provides basic information about CSIRT-PJ, its channels of communication, its roles and responsibilities.

1.1 Date of last update
Version 1, updated on 2017-05-19
Version 2, updated on 2019-01-14

1.2 Distribution list for notifications
There is no distribution list for notification

1.3 Locations where this document may be found
On demand

1.4 Authenticating this document
This document has been signed with the key PGP of CSIRT-PJ, and is available at the following web link:

1.5 Document identification
Title: CSIRT-PJ-RFC2350.pdf
Release 2.0
Date: 01/14/2019
Expiration: this document is valid until superseded by later version.
2 CONTACT INFORMATION

2.1 Team name:
CSIRT-PJ: CSIRT Police Judiciaire

2.2 Address
Ministère de l’Intérieur
Direction Centrale de la Police Judiciaire
Sous-Direction de la Lutte contre la Cybercriminalité
CSIRT-PJ
101 rue des trois Fontanot
92000 NANTERRE
France

2.3 Time zone
CET/CEST  \(\Rightarrow\) UTC/GMT +2 hours (summer: 21st March to September 30th)
CET/CEST  \(\Rightarrow\) UTC/GMT +1 hour (winter: 1st October to March 20th)

2.4 Phone numbers
☎ +33 1 47 44 97 75 (French business hours)
☎ +33 6 88 70 47 17 (obligation H24/7)

2.5 Facsimile number
None available

2.6 Electronic mail address
If anyone need to notify us an information about a security incident or a cyber-threat targeting involving people, SMBs or any other organizations excepted those one which are belonged amongst critical infrastructures sector, we can be contacted at:
✉️: csirt-pj@interieur.gouv.fr

2.7 Other communication means
No

2.8 Encryption information (public key)
CSIRT-PJ as its own PGP Key

Public key fingerprint: \textbf{1258 1F09 6100 B8EA AAD4 611E B932 5D4F 6A36 CF72}
Key ID: 0x6A36CF72

The PGP key can be retrieved from the usual public key servers such as: \url{http://pgp.mit.edu/}
The PGP key shall be used whenever information must be sent to CSIRT-PJ in a secure manner to ensure confidentiality and authentication.
2.9 Team members
CSIRT-PJ team leader is superintendent François BEAUVOIS, and his deputy, Police Captain Christophe MARAIS.

The team is made up of IT security experts.

2.10 Other information
General information about CSIRT-PJ can be found at the following URL:

http://www.police-nationale.interieur.gouv.fr/

2.11 Point of contact
The preferred method to contact CSIRT-PJ is to send an email to the following email address:

✉️: csirt-pj@interieur.gouv.fr

Urgent case can be reported by phone at the following number, H24/7:

📞 +33 6 74 28 05 99

CSIRT-PJ is daily opened between 09:00 AM to 18:00PM, from Monday to Friday. During the weekend CSIRT-PJ is closed but there is an on call system.
3 CHARTER

3.1 Mission statement
CSIRT-PJ is a law Enforcement unit, attached to French Cybercrime Center, depending on the Criminal Investigation Directorate. The core business is the fight against cybercrimes. CSIRT-PJ is based at the crossroad of cybercrime unit and cyber threat intelligence unit.

CSIRT-PJ provides incident response capabilities and tools to investigation units by:
- Providing IR services;
- Providing investigation-related tools;
- Providing expertise through trainings and deliverables;
- Sharing threat intelligence with cybersecurity community.

CSIRT-PJ is a swear unit, driven by several values:

- highest standard of ethics, honesty and professionalism
- committed to deliver a high quality of public services to its constituency
- ensure to respond to security incident as efficiently as possible
- fostering information exchange between CSIRT-PJ and its internal or external relationships

3.2 Constituency
CSIRT-PJ’s constituency is French police investigation units.

3.3 Affiliation
CSIRT-PJ is a governmental service affiliated to French national police. It exchanges at national and international level and develops a security exchange culture that it values.

3.4 Authority
CSIRT-PJ operates under the authority of French interior Minister, in charge of national security as much as common crimes or cybercrimes.
4 POLICIES

4.1 Type of incidents and level of support
CSIRT-PJ is authorized to handle all types of cyberattacks targeting a French victim and for which a case can be opened. Depending on the incident’s type, services roll out its services which include incident response, digital forensics and threat intel analysis. The level of support given by CSIRT-PJ will depend on the severity of the security incident or issue, potential assessed impact and availability of CSIRT-PJ’s resources at the time.

4.2 Co-operation, interaction and disclosure of information
As a Law Enforcement unit, CSIRT-PJ highly considers the paramount importance of operational coordination and information. Due to its status as a LEA, it naturally cooperate and exchanges information in it area of responsibilities.

CSIRT-PJ cooperates with other national Police Unit. It cooperates also with international Law Enforcement organization, for instance European Cyber Crime Centre (EC3) from Europol and of course with Interpol. CSIRT-PJ cooperate and directly exchanges information with the NCFTA (national cybercrime forensics training agency).

CSIR-PJ shares information also between CERTs, CSIRTs, SOCs and similar bodies, and also with other organizations, which may aid to deliver its service.

CSIRT operates within the current French legal framework, and international conventions.

CSIRT-PJ also complies with the CCoP (CSIRT Code of Practice) version 2.1

4.3 Communication and authentication
CSIRT-PJ protects sensitive information in accordance to relevant European regulations and French laws and policies. CSIRT-PJ respects strongly the sensitivity marking given by the information source owners who communicate it to CSIRT-PJ.

Due to the fact CSIRT-PJ is a law enforcement unit, it intrinsically embeds confidentiality and protocols to flag information sensitivity.

Regarding the CSIRT activities, exchanging and communicating incidents information, CSIRT-PJ adopted and implemented in its proceedings the ISTLP (information sharing traffic light protocol; release 1.1)\(^1\)

Communication security is achieved using PGP encryption and authentication depending on the sensitivity level and context.

\(^1\) ISTLP: [https://www.trusted-introducer.org/ISTLPv11.pdf](https://www.trusted-introducer.org/ISTLPv11.pdf)
5 SERVICES

5.1 Announcements
CSIRT-PJ provides and spreads information on the cyber-threat landscape and threat actors’ MO.

5.2 Alerts and warnings
CSIRT-PJ disseminates information about cyber-attacks and threat actors’ MO. Alerts and warnings produced by CSIRT-PJ may be shared and passed on to other CERTs, CSIRTs, SOC or similar bodies if deemed necessary or useful to them.

5.3 Development of security tools
CSIRT-PJ develops security tools in particular to be used by cybercrime investigators to detect malware and find evidences.

5.4 Digital forensics examinations and incident response
CSIRT-PJ performs IR for its constituency. IR aims at identifying evidences in victims computer. CSIRT-PJ performs static and dynamic analysis. Digital forensics is performed as necessary, including hard drive and memory analysis.

6 Incident reporting forms
Forms are used for reporting:
- Incidents related to on-going investigations
- Request for technical support or questions

7 DISCLAIMERS
While every steps of the main role of a CSIRT will be taken, CSIRT-PJ assumes no responsibility for errors or omissions or damages resulting from the use of the information provided.