# EY CSIRT

## RFC 2350

Classification: TLP White

# Content

# 1 Document Information

In accordance with the RFC2350[1], this document contains the description of EYCSIRT, this document lists how to contact the team, and describes its responsibilities and the services offered by our CSIRT.

## 1.1 Review

| Version | Author | Comment | Date |
|---|---|---|---|
| 1.0 | EY CSIRT | Draft of the document | 12/11/2019 |
| 1.1 | EY CSIRT | Update | 15/06/2021 |
| 1.2 | EY CSIRT | Update | 02/05/2022 |

## 1.2 Distribution List for Notifications

There is currently no distribution list for notifications.

For any questions about updates, please send an email to: csirt[at]fr.ey.com

## 1.3 Locations where the document may be found

The latest version of this document is available on EY CSIRT page at
https://www.ey.com/fr_fr/cybersecurity/computer-security-incident-response-team

## 1.4 Authenticating this document

This document has been signed with the PGP key of EYCSIRT.

The PGP public key, ID and fingerprint are available on the EYCSIRT website:
https://www.ey.com/fr_fr/cybersecurity/computer-security-incident-response-team

Fpr: 96F8 8C4D 4E8F 5CBD 8E34 6566 5EC6 931A 1753 2B11
Sub: ECDH/256 Usage: Encrypt Expires: 2024-05-31
UID: EY CSIRT <csirt@fr.ey.com>

## 1.5 Document Identification

Title: EYCSIRT_RFC2350

Version: 1.2

Document date: 02/05/2022

Expiration: This document is valid until superseded by a later version.

# 2 Contact Information

## 2.1 Name of the Team

EYCSIRT

## 2.2 Address

Tour First –

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

1 place des Saisons, TSA 14444

92037, Paris La Défense Cedex 92037

France

## 2.3 Time Zone

CET/CEST, Central European Time or Central European Summer Time, UTC +1/UTC +2

## 2.4 Telephone Number

Phone number: 01 41 44 49 96

## 2.5 Facsimile Number

Not available

## 2.6 Other Telecommunications

Not available

## 2.7 Electronic Mail Address

csirt[at]fr.ey.com

## 2.8 Public Keys and Encryption Information

EYCSIRT uses the following PGP Key:

Fpr: 96F8 8C4D 4E8F 5CBD 8E34 6566 5EC6 931A 1753 2B11
Sub: ECDH/256 Usage: Encrypt Expires: 2024-05-31
UID: EY CSIRT <csirt@fr.ey.com>

## 2.9 Team Members

The EYCSIRT team leader is Marc AYADI.

The members of EYCSIRT team are not publicly available.

## 2.10 Other information

Please see our website: https://www.ey.com/fr_fr/cybersecurity/computer-security-incident-response-team for additional information about EY CSIRT.

## 2.11 Points of Customer Contact

The preferred method of contact is by email to the following address: csirt[at]fr.ey.com.

Specify the nature of the request in the subject field in your email, e.g [URGENT], [Request for information].

EY CSIRT operates 27/7/365.

# 3 Charter

## 3.1 Mission Statement

EYCSIRT will offer assistance to its constituency regarding incident response management from preparation, protection, detection, response and quality improvements.

A dedicated management team is identified with EY cyber teams and will ensure the appropriate communication internally as well as to our constituents. The CSIRT management team also ensures continual improvement of our practices in accordance with standards listed by Trusted Introducer.

EYCSIRT covers multiples areas:

- Digital Forensics and Incidents Responses
- Purple team
- Threat Intelligence

## 3.2 Constituency

EYCSIRT functions are aimed at clients with needs and objectives to address security issues. EY clients are part of private or public organizations.

We also share information and knowledge with EY Lab teams which are continuously working on cybersecurity issues, data analytics and R&D. There are currently 16 Wavespace internationally offering a broad geographic coverage from information gathering to the diffusion of information.

## 3.3 Affiliation

EYCSIRT is part of Ernst & Young Advisory.

## 3.4 Authority

EYCSIRT coordinates security incidents on behalf of its constituency and only at its constituents' request.

EYCSIRT primarily acts as an advisor regarding local security teams and is expected to make operational recommendations. Therefore, EYCSIRT may not have any specific authority to require specific actions. The implementation of such recommendations is not a responsibility of EYCSIRT, but solely of those to whom the recommendations were made.

EYCSIRT will not engage in any contract with CAC customers as legally required.

# 4 Policies

The following sections discuss communication of these policies to the constituent community.

## 4.1 Types of Incidents and Level of Support

EYCSIRT addresses all types of computer security incidents shared with us and which occur, or threaten to occur, in its constituency.

EY team will do everything needed to investigate, advice, contain, remediate and monitor incidents and advise impacted entities.

The level of support provided to our constituency will vary depending on the type and security of the incident, its potential or assessed impact, the type of constituent, the size of the user community affected, the emergency of the situation, the associated SLAs agreed together and the EYCSIRT's resources at the time.

## 4.2 Co-operation, Interaction and Disclosure of Information

EYCSIRT respects the contractual obligations of confidentiality taken with its constituency. No sensitive information is shared without the constituency sponsor's consent.

EYCSIRT considers the importance of operational coordination and information sharing between CERTs, CSIRTs, SOCs and similar entities, and with other organizations, which may aid to deliver its services, or which provide benefits to EYCSIRT's constituency. Consequently, EYCSIRT exchanges all necessary information with affected parties, as well as with other CSIRTs, on a need-to-know basis. However, neither personal nor overhead data are exchanged unless explicitly authorized. More, EYCSIRT will protect the privacy of its customers/constituents, and therefore, under normal circumstances, pass on information in an anonymized way only (unless other contractual agreements apply).

All incoming information is classified by default as "internal". EYCSIRT supports the Information Sharing Traffic Light Protocol version 1.1 (https://www.trusted-introducer.org/ISTLPv11.pdf). Information that comes in with the tags White, Green, Amber or Red will be handled appropriately.

EYCSIRT operates within the current French legal framework.

## 4.3 Communication and Authentication

EYCSIRT protects sensitive information in accordance with relevant regulations and policies with France and the EU.

EYCSIRT supports the Information Sharing Traffic Light Protocol version 1.1 (https://www.trusted-introducer.org/ISTLPv11.pdf). Information that comes in with the tags White, Green, Amber or Red will be handled appropriately.

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

EYCSIRT performs incident response for its constituency.

EYCSIRT handled both the triage and coordination aspects. Incident resolution is left to the responsible administrators within the constituency. However, EYCSIRT will offer support and advice on request. EYCSIRT will assist IT security team in handling the technical and organizational aspects of incidents. In particular, it will provide assistance or advice with respect to the following aspects of incident management.

## 5.1 Incident Response

EYCSIRT incident response team is available 27/7/365 for digital forensics and incident responses mission.

Our process is as followed:

1. Identification and scoping
2. Triage
3. Contain and eradicate
4. Investigation and analysis
5. Remediate and recover
6. Resilience

## 5.2 Incident Triage

- Collect targeted data for initial analysis
- Severity assessment

## 5.3 Incident Coordination

- Incident categorization 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

- Determine tactical recovery actions for client’s environment
- Assist and manage recovery of the client environment
- Empower management to support multiple business recovery agendas

## 5.5 Proactive Activities

- Threat Hunting
- Weekly and monthly cyber threat bulletins
- Continuous monitoring

# 6 Incident Reporting Forms

No local form has been developed to report incidents to EYCSIRT.

In case of an emergency, please provide EYCSIRT with the following information:

- Contact details and organizational information, e.g point of contact or organization name, address and contact information.
- Email address, phone number, PGP key if available.
- Any technical element that may be relevant.

# 7 Disclaimers

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

# EY | Building a better working world

EY exists to build a better working world, helping create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy.



Design Center – 2206DC206
EYG no. 007390-22Gbl

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.



ey.com/fr