

RFC 2350

1. Document Information

This document contains a description of CERT-EU in accordance with RFC 2350¹. It provides basic information about CERT-EU, its channels of communication, and its roles and responsibilities.

1.1. Date of Last Update

Version 5.1 - 2019/09/02

1.2. Distribution List for Notifications

There is no distribution list for notifications.

1.3. Locations where this Document May Be Found

The current version of this document can be found at:

<https://cert.europa.eu/static/RFC2350/RFC2350.pdf>

1.4. Authenticating this Document

This document has been signed with the PGP key of CERT-EU. See section 2.8 for more details.

1.5. Document Identification

Title: "RFC 2350 CERT-EU"

Version: 5.1

Document Date: September 2019

Expiration: This document is valid until superseded by a later version.

2. Contact Information

2.1. Name of the Team

CERT for the EU institutions, bodies and agencies.

Short name: CERT-EU

2.2. Address

CERT-EU
Rue Montoyer 34,
1000 Brussels,
Belgium

2.3. Time Zone

Time-zone: CET/CEST

2.4. Telephone Number

+32 2 299 0005

2.5. Facsimile Number

+32 2 297 9894

2.6. Electronic Mail Address

The preferred method to contact the CERT-EU team for general inquiries is to send an e-mail to the address services@cert.europa.eu which is monitored by a duty officer during hours of operation. Concerning communication on non-operational matters such as administrative activities, send an email to the address secretariat@cert.europa.eu which is operated by the administrative staff of CERT-EU, during office hours.

¹ <http://www.ietf.org/rfc/rfc2350.txt>

Urgent cases can be reported by phone on +32 2 299 0005

Days/Hours of Operation: 09:00 to 17:00, Monday to Friday. Out of office hours' operation in case of emergency.

Use of phone and fax for reporting incidents should be avoided as much as possible.

2.7. Other Telecommunication

None

2.8. Public Keys and Encryption Information

PGP is used for functional exchanges between CERT-EU and its Partners (incident reports, alerts, etc).

Fingerprint: CBD6 07BA 59AC 4462 B98F 8DB2 32AB 2903 830D ACB8

<https://cert.europa.eu/cert/custom/CERT%20for%20the%20European%20Institutions.asc>

2.9. Team Members

The Head of CERT-EU is Saâd Kadhi, the Deputy Head of Unit is Rogier Holla. The team includes 30 staff members.

2.10. Other Information

CERT-EU is member of:

- CNW (EU CSIRTs Network) established with the NIS Directive;
- EGC-Group (European Government CERTs-Group);
- FIRST (Forum of Incident Response and Security Teams);
- TF-CSIRT (Trusted Introducer).

3. Charter

3.1. Mission Statement

CERT-EU's mission is to contribute to the security of the ICT infrastructure of all Union institutions, bodies and agencies ('the constituents') by helping to prevent, detect, mitigate and respond to cyber-attacks and by acting as the cyber-security information exchange and incident response coordination hub for the constituents. The scope of CERT-EU's activities covers prevention, detection, response and recovery.

CERT-EU will operate according to the following key values:

- Highest standards of ethical integrity;
- High degree of service orientation and operational readiness;
- Effective responsiveness in case of incidents and emergencies and maximum commitment to resolve the issues;
- Building on, and complementing the existing capabilities in the constituents;
- Facilitating the exchange of good practices between constituents and peers;
- Fostering a culture of openness within a protected environment, operating on a need-to-know basis.

3.2. Constituency

The constituency of CERT-EU is composed of all the EU institutions, agencies and bodies. For a complete list and more information please see:

http://europa.eu/about-eu/institutions-bodies/index_en.htm

3.3. Sponsorship and/or Affiliation

CERT-EU is sponsored by Commission Vice-President Andrus Ansip and Commissioner for Digital Economy and Society Mariya Gabriel as well as the EU Institutions, Bodies and Agencies.

3.4. Authority

The establishment of the CERT-EU was mandated via Commission decision on 11/11/2012. CERT-EU received a new and permanent legal basis as a result of the inter-institutional Arrangement between the European Parliament, the European Council, the Council of the European Union, the European Commission, the Court of Justice of the European Union, the European Central Bank, the European Court of Auditors, the European External Action Service, the European Economic and Social Committee, the European Committee of the Regions and the European Investment Bank on the organisation and operation of a computer emergency response team for the Union's institutions, bodies and agencies (CERT-EU) on 12/01/2018.

4. Policies

4.1. Types of Incidents and Level of Support

All cyber security incidents are considered normal priority unless they are explicitly labelled EMERGENCY or URGENT.

4.2. Co-operation, Interaction and Disclosure of Information

CERT-EU highly regards the importance of operational cooperation and information sharing between CERTs and NCSCs and also with other organisations which may contribute towards or make use of their services.

CERT-EU operates within the confines imposed by EU legislation.

4.3. Communication and Authentication

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

Communication security (encryption and authentication) is achieved by various means: S/Mime based email encryption (SECEM), PGP, ACID or other agreed means, depending on the sensitivity level and context.

5. Services

5.1. Prevention

This service aims at raising awareness and preventing security events, through issuing advisories and white papers, a security awareness program, security consultation on specific technologies and topics, a portal that includes a security news aggregator and a bug bounty program on vulnerabilities.

5.2. Cyber Threat Intelligence

This service aims at disseminating information on cyber-attacks or disruptions, as well as providing situational awareness and issuing recommendations to the constituents in order to tackle evolving cyber security threats.

5.3 Incident Response

This service aims at specialised investigations and the coordination of response to cyber security incidents in the constituents. The incident support and coordination activities include evaluating available information, validating and verifying it, gathering additional evidence if required, communicating with relevant parties, and finally proposing solutions in order to resolve the incident. In the context of the investigations, forensic, malware network etc. analysis is performed. The service also delivers a number of automated analytical tools to CERT-EU's constituency.

5.4 Monitoring

This service aims at the detection of intrusion events with intrusion detection sensor monitoring and security logs analysis.

5.5 Security Testing

This service aims at the preparation and hardening of constituent's infrastructure, through ethical hacking techniques and customised penetration tests.

6. Incident Reporting

Whenever possible the incidents should be reported to CERT-EU by e-mail using the address: services@cert.europa.eu preferably encrypted with CERT-EU's public key.

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

- Contact details and organizational information – name of person and organisation name and address, email address, telephone number;
- Short summary of the incident/emergency/crisis; type of event;
- Source of indication; (i.e. the system produced an alert etc.);
- System affected; (i.e. network asset etc.);
- Estimated impact; (i.e. loss of communications etc.);
- Other particularities:
 - Details of the observations that led to the discovery of the incident - scanning results (if any); an extract from the log showing the problem, etc.;
 - In case there is a need to forward any emails to CERT-EU, please make sure that all email headers, body and any attachments are included.

7. Disclaimer

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