CERT-EU

RFC 2350

VERSION 5.4 – 2 MARCH 2023

CERT-EU, CERT for the EU Institutions, Bodies and Agencies

Table of Contents

1 Document information

This document contains a description of CERT-EU in accordance with RFC 2350[1]. It provides basic information about CERT-EU, its channels of communication, and its roles and responsibilities.

Date of last update

Version 5.4 – 2 March 2023.

Distribution list for notifications

N/A.

Locations where this document may be found

The current version of this document can be found at:

https://www.cert.europa.eu/files/data/RFC2350.pdf

Authenticating this document

This document has been digitally signed by Saâd Kadhi, the Head of CERT-EU.

Document identification

Title	RFC2350
Version	5.4
Document date	2 March 2023
Expiration	This document is valid until superseded by a later version

2 Contact information

Name of the team

Full name	CERT for the EU institutions, bodies and agencies
Short name	CERT-EU

Address

CERT-EU

Rue de la Loi 107, 1000 Brussels. Belgium.

Time zone

CET/CEST.

Telephone number

+32 2 299 0005.

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

Electronic email address

For notifications, incident reporting and operational matters, please contact us at:

services@cert.europa.eu

This email address is monitored by a duty officer during hours of operation.

For non-operational matters, such as administration-related topics and general inquiries, please send us an email at:

secretariat@cert.europa.eu

This email address is monitored by the administrative staff of CERT-EU during office hours.

In case of an emergency, please contact us by phone at +32 2 299 0005.

Our days/hours of operation are from 09:00 to 17:00 CET/CEST on business days. We may operate out of these hours and days in case of an emergency only.

Other telecommunication

N/A.

Public keys and encryption information

We use PGP for functional exchanges (notifications, incident reporting, etc.) with our peers, partners and constituents.

Fingerprint	4522 E470 EFA2 10AB C77B 6FED A8A6 0841 891D 04EC
Location	https://www.cert.europa.eu/files/data/CERT%20for%20the%20European%20Institutions.asc

Team members

The Head of CERT-EU is Saâd Kadhi. The Deputy Head of CERT-EU is Rogier Holla.

The team includes around 50 staff members.

Other information

CERT-EU is a member of:

- The CSIRTs Network[2] (CNW), which was established by the NIS Directive.
- The European Government CERTs (EGC) group[3].
- FIRST[4], the Forum of Incident Response and Security Teams.
- TF-CSIRT[5], the Task Force on Computer Security Incident Response Teams.

[2] https://csirtsnetwork.eu/

[3] https://egc-group.org/

[4] https://www.first.org/members/teams/cert-eu

[5] https://www.trusted-introducer.org/directory/teams/cert-eu.html

3 Charter

Mission statement

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

We operate according to the following key values:

- The highest standards of ethical integrity.
- A high degree of service orientation and operational readiness.
- An effective responsiveness in case of cybersecurity incidents and emergencies and the highest level of commitment to resolve the issues.
- Building on, and complementing the existing capabilities of our constituents.
- Facilitating the exchange of good practices among our constituents and with our peers.
- Fostering a culture of openness within a protected environment, operating on a need-to-know basis.

Constituency

The constituency of CERT-EU is composed of all the EU institutions, agencies and bodies.

For a complete list and more information, please refer to:

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

Sponsorship and/or affiliation

CERT-EU is a Task Force of the European Commission with an inter-institutional mandate.

Authority

The establishment of CERT-EU was mandated by a European Commission decision on 11 November 2012.

CERT-EU received a new and permanent legal basis as a result of the Inter-Institutional Arrangement[6] 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 January 2018.

4 Policies

Types of incidents and level of support

All cybersecurity incidents will be given normal priority unless they are explicitly labelled **EMERGENCY** or **URGENT**.

Co-operation, interaction and disclosure of information

CERT-EU highly regards the importance of operational cooperation and information sharing between CSIRTs, 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.

[6] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018Q0113(01)&from=EN

Communication and authentication

CERT-EU protects sensitive information in accordance with the relevant regulations and policies within the EU.

In particular, CERT-EU respects the sensitivity markings defined by the 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 or other agreed means, depending on the sensitivity level and context.

5 Services

Identify (ID)

This service aims at identifying and managing cybersecurity risks. It creates a vulnerability knowledge base through external network scans, exposure assessment and a coordinated vulnerability disclosure mechanism, which then feeds our constituents through advisories and vulnerability alerts.

Moreover, it consists of regular and ad hoc reporting of threat information. It also aids the preparation and hardening of our constituency's infrastructure, through ethical hacking techniques, vulnerability assessments, phishing exercises, customised penetration tests and Red Team exercises.

The overall preparedness to face a wide range of threats is complemented by cyber exercises and the implementation of after-action reports.

Protect (PR)

This service aims at raising cybersecurity awareness and improving prevention through the issuance of guidance documents and threat heads-up, conducting cybersecurity awareness sessions and technical assessments of constituents' infrastructure.

Detect (DE)

This service aims at the detection of possible cyber-attacks through intrusion detection monitoring and security log collection and analysis.

Respond (RS)

This service aims at specialised investigations and response coordination to cybersecurity incidents impacting our constituency.

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 to resolve the incident.

In the context of the investigations, digital forensics and artefact analysis may be performed. The service also delivers a number of automated analytical tools to our constituency.

Lastly, it establishes and makes use of a crisis response management plan.

Recover (RC)

This service aims at supporting our constituents develop and implement the right measures in order to mitigate the effects of an incident. It entails the provision of guidelines for customised incident response plans, specific recovery recommendations, lessons learned, as well as coordination of communications.

6 Incident reporting

Whenever possible, incidents should be reported by email at services@cert.europa.eu, preferably encrypted with our PGP public key.

When you contact us, please provide at least the following information:

1. Contact details and organisational information — name of person, organisation name and address, email address, telephone number.
2. Short summary of the incident / emergency / crisis and type of event.
3. The event / incident source (e.g. which system produced an alert).
4. Affected system(s).
5. Estimated impact (e.g. loss of communications).
6. Additional information such as 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 you need to forward any suspicious emails to us, please make sure that all email headers, body and any attachments are included.

CERT-EU uses the Reference Security Incident Classification Taxonomy.

7 Disclaimer

While every precaution is 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.

CERT-EU

Digitally signed by:
SAÂD KADHI (EUROPEAN COMMISSION)
Date: 2023-03-02 16:37:11 UTC

CERT-EU

THINK CONSTITUENT
CREATE VALUE

https://cert.europa.eu

services@cert.europa.eu