computer emergency response team CERT-EU

RFC 2350

1. Document Information

This document contains a description of CERT-EU in according to RFC 2350[1]. It provides basic information about the CERT-EU Pre-Configuration team, its channels of communication, and its roles and responsibilities.

1.1. Date of Last Update

Version 1.0 2011/10/25

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 always be found at http://cert.europa.eu.

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: 1.0
Document Date: October 2011
Expiration: This document is valid until superseded by a later version

2. Contact Information

2.1. Name of the Team

CERT-EU Pre-Configuration Team
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

+3222990005

2.5 Facsimile Number

+32 2 297 9894

2.6 Electronic Mail Address

All incidents reports should be sent to cert-eu@ec.europa.eu
Use of phone and fax for reporting incidents should be avoided as much as possible.

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

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).

ID
0x46AC4383
(0x78CCB868 encryption subkey)
(0xC8F12568 signing subkey)

Fingerprint: 9011 6BE9 D642 DD93 8348 DAFA 27A4 06CA 46AC 4383

2.9 Team Members
The CERT-EU team leader is Freddy Dezeure. The team is made up of IT security experts from the main EU Institutions (European Commission, General Secretariat of the Council, European Parliament, Committee of the Regions, Economic and Social Committee) and ENISA.

2.10 Other Information

2.11 Points of Customer Contact
The preferred method to contact CERT-EU Pre Configuration team is to send an e-mail to the address cert-eu@ec.europa.eu which is monitored by a duty officer during hours of operation.

Urgent cases can be reported by phone on +3222990005

Days/Hours of Operation: 09:00 to 17:00 Monday to Friday

3. Charter

3.1 Mission Statement
CERT-EU's mission is to support the European Institutions to protect themselves against intentional and malicious attacks that would hamper the integrity of their IT assets and harm the interests of the EU. 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 with peers
- Fostering a culture of openness within a protected environment, operating on a need to know basis

3.4 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

3.5 Sponsorship and/or Affiliation
CERT-EU is sponsored by Commission vice-President Neelie Kroes and Commission vice-President Maroš Šefčovič, EU Institutions, Bodies and Agencies.

3.6 Authority
The establishment of the CERT-EU Pre Configuration Team was mandated via document 10539/11

4. Policies

4.1 Types of Incidents and Level of Support

The pre-configuration team will gradually roll out its services, starting with Announcements, Alerts and Incident Response Coordination (see 5 below)

4.2 Co-operation, Interaction and Disclosure of Information

CERT-EU highly regards the importance of operational cooperation and information-sharing between Computer Emergency Response Teams, 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 or ACID or other agreed means, depending on the sensitivity level and context.

5. Services

5.1 Announcements

This service aims at providing information (e.g. on threat landscape, published vulnerabilities, new attack tools or artefacts, security/protection measures, etc.) needed to protect systems and networks.

5.2 Alerts and warnings

This service aims at disseminating information on cyber attacks or disruptions, security vulnerabilities, intrusion alerts, computer viruses, and providing recommendations to tackling the problem to the constituent.

5.2 Incident Response Coordination

This service aims at the coordination of response to information security incidents in the institutions and bodies of the European Union, in cooperation with the owners and providers of impacted parts of the the respective IT infrastructure, the European and international communities of Computer Emergency Response Teams, telecommunication operators, ISPs and other public and private bodies (police, investigators, courts) as appropriate

6. Incident Reporting Forms

A standard incident reporting form is available from http://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_11_002_v2_1.pdf. Whenever possible, this from should be completed and sent to CERT-EU.

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

- contact details and organizational information – name of person and organisation name and address, email address, telephone number;
- IP address and observation;
- scanning results (if any) - an extract from the log showing the problem;
- In case you wish to forward any emails to CERT-EU, please make sure that all email headers, body and any attachments are included.

7. Disclaimers

CERT-EU, the CERT for the EU institutions, is currently in its setup phase until May 2012. Services are provided in a pilot fashion, and are not yet fully functional. Announcements, alerts and warnings are sent out in best effort manner, and to contact information currently known to us. 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.