



CERT-RO – Romanian National Computer Emergency Response Team

RFC 2350 description for CERT-RO

(Romanian National Computer Emergency Response Team)

1. Document Information

This document contains a description of CERT-RO in according to RFC 23501, providing basic information about the CERT-RO team, its channels of communication, its roles and responsibilities.

1.1 Date of Last Update

This is version 1.0, published January 2012.

1.2 Distribution List for Notifications

For the moment there is no distribution list for notifications yet

1.3 Locations where this Document May Be Found

The current version of this document can be found at:

<http://www.cert-ro.eu/files/doc/RFC2350.pdf>.

1.4 Authenticating this Document

This document have been signed with the CERT-RO's PGP key. The signatures are also on our Web site, at <http://www.cert-ro.eu/contact.php>.

2. Contact Information

2.1 Name of the Team

Romanian Computer Emergency Response Team

Short name: CERT-RO

2.2 Address

CERT-RO

8-10 Maresal Averescu Ave.
011455 Bucharest
Romania

2.3 Time Zone

EET – Eastern European Time (UTC/GMT + 2 hours)

2.4 Telephone Number

+4 031 620 2180

2.5 Facsimile Number

+4 021 316 0764

2.6 Electronic Mail Address

Office: office@cert-ro.eu

Incident Reports: alerts@cert-ro.eu.

2.7 Other Telecommunication

N/A.

2.8 Public Keys and Other Encryption Information

The CERT-RO has a PGP key, whose details are:

User ID: CERT-RO Alerts < alerts@cert-ro.eu >
Key ID: 0xFE3ABF1C Key type: RSA
Key size: 2048 Expiration: 14.10.2016
Fingerprint: 827D 41E9 AE80 03B7 92F5 48EE 82D2 073B FE3A BF1C

The key and its signatures can be found at the usual large public key-servers.

2.9 Other Information

General information about CERT-RO can be found at <http://www.cert-ro.eu>.

2.10 Points of Customer Contact

The preferred method for contacting CERT-RO is via e-mail at:

- office@cert-ro.eu for general purposes, and
- alerts@cert-ro.eu for incident reports.

3. Charter

3.1 Mission Statement

CERT-RO is the National CERT of Romania, established as an independent structure for research, development and expertise in the field of cyber-security. It is a specialized organization responsible for preventing, analyzing, identifying and reacting to cyber-incidents. CERT-RO is the national contact point for similar structures. CERT-RO is responsible for elaborating and distributing public politics for prevention and counteracting the incidents that occur within national cyber infrastructures.

3.2 Constituency

The CERT-RO constituency is composed of all users, systems and networks from Romanian cyber-space.

3.3 Sponsorship and/or Affiliation

CERT-RO is established as a Romanian governmental institution for research, development and expertise in the field of cyber-security.

3.4 Authority

The establishment of CERT-RO was mandated via Romanian government decision H.G. 494 / 11 May 2011.

4. Policies

4.1 Types of Incidents and Level of Support

CERT-RO is authorized to address all types of computer security incidents which occur, or threaten to occur, in Romanian cyber-space.

The level of support given by CERT-RO will vary depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected, and the CERT-RO's resources at the time, though in all cases some response will be made within 24 hours during working days.

Incidents will be prioritized according to their apparent severity and extent. Note that no direct support will be given to end users; they are expected to contact their system administrator, network administrator, or department head for assistance.

4.2 Co-operation, Interaction and Disclosure of Information

CERT-RO highly regards the importance of operational cooperation and information-sharing between Computer Emergency Response Teams, and also with other organizations which may contribute towards or make use of their services.

CERT-RO is a member of TF-CSIRT community and communicate and cooperate with other CSIRTs.

CERT-RO exchanges all necessary information with other CSIRTs as well as with affected network/services administrators.

All sensitive data and information (personal data, system/service configuration, vulnerabilities with their locations) are transmitted encrypted.

CERT-RO operates within the confines imposed by Romanian and European legislation.

4.3 Communication and Authentication

In view of the types of information that the CERT-RO will likely be dealing with, telephones and unencrypted e-mail will be considered sufficiently secure for the transmission of low-sensitivity data.

If it is necessary to send highly sensitive data by e-mail, PGP encryption will be used.

Where it is necessary to establish trust, for example before relying on information given to the CERT-RO, or before disclosing confidential information, the identity and bona fide of the other party will be ascertained to a reasonable degree of trust.

Appropriate methods for trust establishment will be used, such as a search of FIRST members, the use of WHOIS and other Internet registration information etc., along with telephone call-back or e-mail mail-back to ensure that the party is not an impostor. Incoming e-mail whose data must be trusted will be checked with the originator personally, or by means of digital signatures (PGP in particular is supported).

5. Services

5.1 Incident Response

CERT-RO will handle the technical and organizational aspects of incidents. In particular, it will provide assistance or advice with respect to the following aspects of incident management:

5.1.1 Incident Triage

- Investigating whether indeed an incident occurred;
- Assessing and prioritizing the incident;
- Conducting investigation.

5.1.2 Incident Coordination

- Determining the involved organizations;
- Contact the involved organizations to investigate the incident and take the appropriate steps;
- Facilitate contact to other parties which can help resolve the incident;
- Contacting or facilitating contacting appropriate law enforcement officials, if necessary.

5.1.3 Incident Resolution

- Technical assistance and analysis of compromised systems.
- Support in restoring affected systems and services to their previous status.
- Collecting statistics and evidence about incidents, that could be used for protecting against future attacks.

5.2 Proactive Activities

The CERT-RO coordinates and maintains the following services to the extent possible depending on its resources:

- Informational and educational events;
- Records of security incidents handled will be kept;
- Auditing services.

6. Incident Reporting Forms

There are no local forms developed yet for reporting incidents to CERT-RO. Incident reports can be sent to alerts@cert-ro.eu. Please make sure that your incident report contains:

- Your contact and organizational information - name and organization name, email, telephone number;
- IP address and case type;
- A cut from a log showing the problem;
- A copy of the full mail-header from the e-mail which is considered to be a spam or virus;
- A report about phishing or pharming must contain URL, and source of the web page if possible.

7. Disclaimers

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