RoCSIRT Service Definition

Manuel Șubredu

26 November, 2013

1. Foreword

This document is based on BELNET CERT Service Definition document, available on http://cert.belnet.be/. It describes the services proposed by RoCSIRT, under the hood of Agency ARNIEC (former O.A.O.I.C.D. RoEduNet), the Romanian National Research & Education Network.

2. Document information

2.1. Date of last update

Version 1.04: June 2012

2.2. Distribution List for Modifications

Notifications are sent by using our announcements mailing list: announces@csirt.ro . The mailing list information with archives and subscription form can be found at https://www.csirt.ro/mailman/listinfo/announces

2.3. Locations where this document may be found

The current version of this document is available on the RoCSIRT web site: https://www.csirt.ro/

2.4. Authenticating this document

The PDF version of this document has been digitally signed with the RoCSIRT PGP key. This signature can be found alongside the document, on the web site: http://www.csirt.ro/ . Given the difficulty in reliably signing web pages, the HTML versions are not digitally signed.

3. Contact Information

3.1. Name of the team

RoCSIRT complete and official name is: Agency ARNIEC Computer Security Incident Response Team.

3.2. Postal address

RoCSIRT
Agency ARNIEC/RoEduNet
Mendeleev, 21-25
010362 Bucharest
Romania

3.3. Timezone

Eastern European Time (GMT+0200 in winter time, GMT+0300 during the daylight saving period)

3.4. Telephone number

+40 213 171 174

3.5. Fax number

+40 213 171 174

3.6. Email

team@csirt.ro

3.7. PGP keys

3.7.1. RoCSIRT team key - team@csirt.ro

This key is to be used for any confidential communication with RoCSIRT: reporting vulnerabilities, incidents, questions, etc. This key will also sign any official communication, except advisories.

Key Id 0x58768017
Key Type DH-1024
Key Fingerprint 4386 9EC9 60AA C18C A6B9 5425 A5B4 6EC1 5876 8017

3.7.2. Team members and collaborators

Manuel ȘUBREDU (manuel.subredu@roedu.net)
PGP Key 0x2BDCDC0B
PGP Key Type DH-1024
PGP Key Fingerprint 74FE 1633 421A 6FB0 4D59 15A0 8C65 DB51 2BDC DC0B

Mihai BĂRBULESCU (mihai.barbulescu@roedu.net)
PGP KEY 0x5F5818F9
PGP Key Type 2048R
PGP Key Fingerprint B2E7 B56E A545 F305 931C FE96 CEC7 9D72 5F58 18F9

Hadrian-Dan POPESCU (adip@roedu.net)
PGP Key 0x5BED3077
PGP Key Type DH-1024
PGP Key Fingerprint 29B6 620E 9163 D9EC 89D9 0A7F E5F6 3347 5BED 3077

Adrian ISTRATE (adrian.istrate@roedu.net)
PGP Key 0x92A966B5
PGP Key Type DH-1024
PGP Key Fingerprint ADD9 5D32 20EF 5F37 60C4 F7B0 71C4 D200 92A9 66B5

Florin PETRE (florin.petre@roedu.net)
PGP Key 0x6F8FAA2F
PGP Key Type DH-1024
PGP Key Fingerprint 4B7A 0B3E 6EE2 7ADE 0AEA 3C47 6536 AA03 6F8F AA2F

Raul OPRUTA (raul.opruta@roedu.net)
PGP Key 0x6237E8B8
PGP Key Type DH-1024
PGP Key Fingerprint CE9C 7746 23CD 1CEA 16A0 28BE E2D2 F4DE 6237 E8B8

Valeriu VRACIU (valeriu@roedu.net)
PGP Key 0xAB58F78F
PGP Key Type DH-1024
PGP Key Fingerprint 6068 8F73 CA32 AB67 0540 0B3C 9DC2 3E09 AB58 F78F

3.8. Points of Contacts

Preferred method to contact us is by email. If it is not possible, we can be reached by phone, during office hours 8:00 – 16:00, from Monday to Friday (legal holidays excluded).

4. Charter

4.1. Mission Statement

The Primary purpose of RoCSIRT is to provide a mechanism for institutions connected to RoEduNet to deal with computer security problems and their prevention. We can consider 2 main goals:

1. handle security incidents and solve security problems occurring within the RoEduNet operated network and systems;
2. warn and educate systems administrators and users by means of information distribution.

4.2. Constituency

RoCSIRT constituency is formed by all RoEduNet connected institutions (research centers, universities, high schools, primary schools, etc) that will be named from this point forward, institutions. Additionally, RoCSIRT may provide CSIRT services to other entities within Romania. Those entities will be considered by RoCSIRT as an integrating part of its constituency if they comply with specific conditions related to sensitive information handling. The complete and updated constituency information will be available on the RoCSIRT website.

RoEduNet connected institutions are exported under the following AS list: AS2614, AS3233, AS6693, AS9199, AS12356, AS12675, AS13210, AS16120, AS16220, AS20820, AS24839, AS25278, AS25304, AS39815, AS42142, AS43703, AS49437, AS49507, AS50940, AS50944, AS51098, AS57444, AS61353, AS199513. The same list can be found on RIPE AS-ROEDUNET object and should be synced with the above ASNs.

RoCSIRT will receive intrusions attempts reports, virus incidents and other security problems from defined staff of each customer within each institution, namely Security Contact Person(s).

Institutions connected to RoEduNet will automatically benefit from the RoCSIRT services, at no extra charges.

4.3. Funding

RoCSIRT is a virtual, physically distributed team within Agency ARNIEC. The funding of RoCSIRT is part of general Agency ARNIEC funding.

RoCSIRT will establish and maintain already existing affiliations with other CERT/CSIRT around the world.

4.4. Authority

RoCSIRT operates under the auspices of Agency ARNIEC (former O.A.O.I.C.D. RoEduNet), the Romanian National Research and Education Network. The Agency ARNIEC network is called RoEduNet. As such, its authority is that given by Agency ARNIEC Acceptable Use Policy (AUP), which is part of Agency ARNIEC General Conditions. Thereby RoCSIRT works cooperatively with its constituency's security teams.

5. RoCSIRT Policies

5.1. Types of incidents and level of support

RoCSIRT is authorized to address all types of computers security incidents that occur at its constituency.

RoCSIRT may act upon requests of one of its constituents or may act if one of its constituents is involved in a computer security incident.

The level of support given by RoCSIRT will vary depending of the type and severity of the incidents or issues, the size of the user community affected and the RoCSIRT's resources at the time, though in all cases some response will be made available within one working day.

The following incidents will be handled by RoCSIRT (list in decreasing order of priority):

1. direct attack on any server/system or network equipment that is part of RoEduNet's backbone network infrastructure;
2. root/system-level attack on any public servers;
3. any other type of compromise which lead or may lead to unauthorized access of Agency ARNIEC equipments;
4. (Distributed) Denial Of Service (D-DOS) on any of the above 3 items;
5. any kind of the previous malicious actions originating from the constituency of RoCSIRT;
6. large scale attacks (not including DDOS) of any kind (sniffing, password attacks...);
7. abusive use of network infrastructure to diffuse criminal or offensive material (child pornography, terrorist or racists messages, ...).

Other types of incidents will be prioritized according to their apparent severity and extent. The relative severity of incidents will be assessed at RoCSIRT's discretion.

RoCSIRT will in principle accept any incidents reports that involve a member of the constituency, either as victim or as suspect.

Incidents reports from individual users will be given a low priority and will be deferred to their responsible security authority.

5.2. Co-operation, Interaction and Disclosure of Information

While there are legal and ethical restrictions on the flow of information from RoCSIRT, all of which may also be outlined in Policies at the organizations of its constituency, and all of which will be respected, RoCSIRT acknowledges its indebtedness to, and declares its intention to contribute to, the spirit of cooperation that created the Internet. Therefore, while appropriate measures will be taken to protect the identity of members of our constituency and members of neighboring sites where necessary, RoCSIRT will otherwise share information freely when this will assist others in resolving or preventing security incidents.

In the paragraphs below, "affected parties" refers to the legitimate owners, operators, and users of the relevant computing facilities. It does not refer to unauthorized users, including otherwise authorized users making unauthorized use of a facility; such intruders may have no

expectation of confidentiality from RoCSIRT. They may or may not have legal rights to confidentiality; such rights will of course be respected where they exist. RoCSIRT may release information to any third party or to governing authorities whenever there is a legal obligation to do so. However, RoCSIRT may in some cases delay this action until such a circumstance has been established irrevocably, e.g. by court order. RoCSIRT will in such cases always notify the affected persons or organizations.

Information being considered for release will be classified as follows:

- Private user information - information about particular users, or in some cases, particular applications, which must be considered confidential for legal, contractual, and/or ethical reasons; private user information will not be released in identifiable form outside RoCSIRT, except as provided for below. If the identity of the user is disguised, then the information can be released freely (for example to show a sample .cshrc file as modified by an intruder, or to demonstrate a particular social engineering attack).
- Intruder information is similar to private user information, but concerns intruders; while intruder information, and in particular identifying information, will not be released to the public (unless it becomes a matter of public record, for example because criminal charges have been laid), it will be exchanged freely with system administrators and CSIRTs tracking an incident.
- Private site information is technical information about particular systems or sites; it will not be released without the permission of the site in question, except as provided for below.
- Vulnerability information is technical information about vulnerabilities or attacks, including fixes and workarounds. Vulnerability information will be released freely, though every effort will be made to inform and work with the relevant vendor before the general public is informed.
- Embarrassing information includes the statement that an incident has occurred, and information about its extent or severity. Embarrassing information may concern a site or a particular user or group of users; embarrassing information will not be released without the permission of the site or users in question, except as provided for below.
- Statistical information is embarrassing information with the identifying information stripped off. Statistical information will be released at the discretion of RoCSIRT.
- Contact information explains how to reach Security Contact Persons and CSIRT's. Contact information will be released freely to members of the constituency, except where the contact person or entity has requested that this not be the case, or where RoCSIRT has reason to believe that the dissemination of this information would not be appreciated.

5.2.1. Potential recipients of information

Potential recipients of information from RoCSIRT will be classified as follows:

1. Members of the constituency's management
2. Security contact persons at organizations
3. Users within the constituency
4. Constituency community
5. Public at large

6. Computer security community
7. Press
8. Other sites and CSIRT's
9. Vendors
10. Law enforcement

Members of the constituency's management

Due to the nature of their responsibilities and consequent expectations of confidentiality, members of the constituency's management are entitled to receive whatever information is necessary to facilitate the handling of computer security incidents that occur in their jurisdictions.

Security Contact Persons at organizations

Security Contact Persons at organizations that are members of the constituency are also, by virtue of their responsibilities, trusted with confidential information. However, unless such people are also members of RoCSIRT, they will be given only that confidential information which they must have in order to assist with an investigation, or in order to secure their own systems.

Users within the constituency

Users within the constituency should have as little interaction with RoCSIRT as possible. Instead, their primary point of contact should be their parent institution's security team that in turn would contact RoCSIRT, if necessary.

The constituency community

The constituency community will receive no restricted information, except where the affected parties have given permission for the information to be disseminated. Statistical information may be made available to the general community. There is no obligation on the part of RoCSIRT to report incidents to the community, though it may choose to do so; in particular, it is likely that RoCSIRT will inform all affected parties of the ways in which they were affected, or will encourage the affected site to do so.

The public at large

The public at large will receive no restricted information. In fact, no particular effort will be made to communicate with the public at large, though RoCSIRT recognizes that, for all intents and purposes, information made available to its constituency community is in effect made available to the community at large, and will tailor the information in consequence.

The computer security community

The computer security community will be treated the same way the general public is treated. While members of RoCSIRT may participate in discussions within the computer security community, such as newsgroups, mailing lists (including the full-disclosure list "bugtraq"), and conferences, they will treat such forums as though they were the public at large. While technical issues (including vulnerabilities) may be discussed to any level of detail, any examples taken from RoCSIRT experience will be disguised to avoid identifying the affected parties.

The press

The press will also be considered as part of the general public. RoCSIRT will generally not interact directly with the Press concerning computer security incidents, except to point them toward information already released to the general public. However, RoCSIRT acknowledges the role of the Press as a vehicle to inform the broad public in general and its own constituency in particular. To properly accommodate this function, the Agency ARNIEC Public Relations department acts as the focal point .

In press contacts, the Agency ARNIEC Public Relations department will call in RoCSIRT in case a RoCSIRT statement is needed. Only RoCSIRT can make statements on behalf of RoCSIRT. The General Manager, the deputy General Manager of Agency ARNIEC, and the CSIRT Coordinator are responsible for making public statements on behalf of RoCSIRT. The above does not affect the ability of individual members of RoCSIRT to grant interviews on general computer security topics; in fact, they are encouraged to do so, as a public service to the community. Note that all RoCSIRT members are committed to absolute confidentiality pertaining specific incidents.

Other sites and CSIRTs

Other sites and CSIRTs, when they are partners in the investigation of a computer security incident, will in some cases be trusted with confidential information. This will happen only if the other site's bona fide can be verified, while the transmitted information will be limited to that which is likely to be helpful in resolving the incident. Such information sharing is most likely to happen in the case of sites well known to RoCSIRT (for example, several other European CSIRT's may have informal but well established working relationships with RoCSIRT in such matters). For the purpose of resolving a security incident, otherwise semi-private but relatively harmless user information, such as the provenance of connections to user accounts, will not be considered highly sensitive and can be transmitted to a foreign site without excessive precautions. "Intruder information" will be transmitted freely to other Security Contact Persons and CSIRT's. "Embarrassing information" can be transmitted when there is reasonable assurance that it will remain confidential and when it is necessary to resolve an incident.

In its contact with other CSIRT's, RoCSIRT will ensure that the information made available to others will be signed (so as to provide for non-repudiation), and, whenever deemed necessary, encrypted. See also 4.3 for more details.

Vendors

Vendors will be considered as foreign CSIRT's for most intents and purposes. RoCSIRT wishes to encourage vendors of all kinds of networking and computer equipment, software, and services to improve the security of their products. In aid of this, a vulnerability discovered in such a product will be reported to its vendor, along with all technical details needed to identify and fix the problem. Identifying details will not be given to the vendor without the permission of the affected parties.

Law enforcement officers

Law enforcement officers will receive full cooperation, as permitted by law, from RoCSIRT, including any information they require to pursue an investigation, notwithstanding the earlier statements made about confidentiality.

5.3. Communication and Authentication

In view of the types of information that RoCSIRT will likely be dealing with, telephones will be considered sufficiently secure to be used even unencrypted. Unencrypted e-mail will not be considered secure, but will be sufficient for the transmission of low-sensitivity data. If it is necessary to send highly sensitive data by e-mail, PGP (with encryption) will be used. Network file transfers will be considered to be similar to e-mail for these purposes: sensitive data should be encrypted before transmission.

When it is necessary to establish trust, for example before relying on information given to RoCSIRT, or before disclosing confidential information, the identity and bona fide of the other party will be ascertained to a reasonable degree of trust. Within the constituency, and with known neighbor sites, referrals from known trusted people will suffice to identify someone. Otherwise, appropriate methods 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).

5.3.1. Data protection

All data (email messages, files, documents etc) that is received or generated by RoCSIRT will be grouped into the following categories:

1. Public
2. Internal
3. Confidential
4. Strictly Confidential

All data, regarding of category (excluding public data), will be subject of access control and authorization.

Public data

This is data that have no impact on RoEduNet or its constituents. This type of data has no special treatment and can be stored on any computer or device.

Internal data

Internal data is Information about RoEduNet and Agency ARNIEC including but not limited to: personnel information, network information, data or architecture and any other kind of data that involves or is about Agency ARNIEC and RoEduNet.

The target of Internal data is only RoEduNet personnel. Internal data will be stored only on work computers or RoEduNet servers or services. Internal data will not be transferred or stored on equipment or services that do not belong to RoEduNet. Internal data is the data that involves

Confidential data

All data that RoCSIRT receives or generates trough the use of specific systems and services is considered confidential data. Confidential data is considered to have a significant impact on RoEduNet or its constituents, systems and networks.

Access to confidential data will be granted only to RoCSIRT team members and it will be stored only on RoCSIRT specific equipment and services. It is recommended that all confidential data to be encrypted at rest and decrypted only on a need to use basis. If parts of

that data need to be transmitted to a constituent or to third parties, RoCSIRT will first try to send the data using secured encrypted channels.

When encrypted channels are not an option, RoCSIRT will consider two sub-types of data: data that refers or implies RoEduNet or his constituents, and data that refers to third parties. Confidential data that involves in any way RoEduNet or constituents will be sent through unencrypted channels only and only if the recipient is a person (not an alias, group or mailing list) and only if the data transits only RoEduNet. Regarding the other category (data involving third parties) RoCSIRT can use unencrypted channels if the recipient explicitly approves that means of communication.

Strictly confidential data

All confidential data that has high impact on RoEduNet, constituent or third party systems or services will be considered strictly confidential data.

Access to this kind of data will be granted on a case-by-case scenario according to specific needs. When needed, not all RoCSIRT team members may have knowledge of that data (the actual data or the fact that it even exists).

All information will be stored only in encrypted form and only on specific, encrypted devices like secure USB flash memory or secured hard-disk drives. Disclosure of this type of data will be possible on a case-by-case basis and only by the RoCSIRT coordinator. If the data involves in any way RoEduNet equipment or constituents, that data may be shared with Agency ARNIEC / RoEduNet decision factors (General Manager, Deputy General Manager, CTO).

5.3.2. Data retention

Usually, if possible, all data shall be in electronic form and it must be treated according to Data protection chapter. Regarding the category in which the data falls, the following conditions must be met when retaining the electronic data:

1. Data will not be stored in any way using public services like clouds;
2. Data will not be associated with personal accounts;
3. Data will not be stored on personal devices (laptops, tablets, etc)

All backups of the electronic data will be made only by appointed personnel and only on secured, private RoEduNet equipment. Access to that equipment will be strictly restricted and only the authorized personnel will have access to the system. When doing/copying backups on external medium (DVDs, BluRay, etc) all RoCSIRT data will be excluded from the backup. Under no circumstances RoCSIRT data should be stored on external medium.

When dealing with paper data, all papers will be scanned and the physical medium should be destroyed using paper shredders.

5.3.3. Data destruction

All hardcopy information (paper or optical disks) should be destroyed as soon as they are no longer needed, using specialized shredders, by the last person that had access.

When dealing with electronic data and information, disks should be erased using at least secure erasing software. If possible, mechanical destruction of disks using specialized equipment is preferred.

6. Services

6.1. Reactive Services

These services are offered in reaction to an occurring incident, be it detected by Agency ARNIEC/RoEduNet staff or a constituency's staff. They focus on short-term issues.

6.1.1. Alerts and Warnings

RoCSIRT will provide its constituency with information about ongoing attacks, security vulnerabilities, alerts in the general sense, and short-term recommended course of action for dealing with the resulting problems.

6.1.2. Incident Handling

RoCSIRT will assist its constituency 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 handling.

Incident Triage

- assessing whether indeed an incident occurred;
- determining the extent of the incident.

Incident Response

RoCSIRT will only provide incident resolution service for Agency ARNIEC / RoEduNet's own systems:

- removing the vulnerability;
- securing the system from the effects of the incident;
- evaluating whether CSIRT actions aimed at an eventual prosecution or disciplinary action are suitable: collection of evidence after the fact, observation of an incident in progress, setting traps for intruders, etc.
- collecting evidence where criminal prosecution or disciplinary action is contemplated.

RoCSIRT will not provide incident resolution service to its customers, as it is left to discretion of local security teams.

Incident Response Coordination

- if possible, determining the initial cause of the incident (vulnerability exploited);
- facilitating contact with other sites which may be involved;
- facilitating contact with Agency ARNIEC Institution Security Teams and/or appropriate law enforcement officials, if necessary;
- making reports to other CSIRT's;
- composing announcements to users, if applicable.

6.1.3. Vulnerability Handling

RoCSIRT will assist its constituency in reaction to the discovery of new vulnerabilities.

Vulnerability Response Coordination

RoCSIRT will help its constituency to determine the proper action to conduct when discovering a vulnerability. This involves

- vendor notification;
- communication with other CSIRT's;

- communication with other institutions Security Teams;
- composing announcements to users, if applicable.

6.1.4. Artifact Handling

An artifact is any file or object found on a system that might be involved in probing or attacking systems and networks, or that can be used to defeat security measures. Examples of artifacts are viruses, Trojan horse programs, worms, exploit scripts, root kits, etc.

Artifact Analysis

RoCSIRT will perform limited technical examination and analysis of any artifact found on a system and/or submitted by one of its constituents:

- file type identification;
- comparison with existing artifacts;
- searching trough online databases of artifacts;
- feeding the artifact to sandbox services;

Artifact Response Coordination

RoCSIRT will help its constituency to determine the proper action to conduct when faced with artifacts. This involves:

- share analysis reports with other CSIRT's, vendors, experts;
- notification of other parties;
- synthesizing analysis from various sources;
- maintaining a constituents accessible archive of artifacts and corresponding response strategies.

6.2. Proactive Services

These services aim to prevent incidents from happening and reduce their impact when they occur. They focus on medium- to long-term issues.

6.2.1. Announcements

Announcements include

- intrusion alerts;
- vulnerability warnings;
- security advisories.

These announcements inform the constituents about new developments with medium to long-term impact, in order to enable them to protect their systems against newly found problems before they can be exploited.

6.2.2. Technology Watch

RoCSIRT monitors and observes new technical developments, intruder activities and related trends.

6.2.3. Configuration of Tools

RoCSIRT helps its constituency to configure security-related tools by providing sample configuration of typical tools or sample secure configuration of widely used tools, such as mail, DNS or web servers.

6.2.4. Security-Related Information Dissemination

RoCSIRT will provide a collection of useful information that aids in improving security. Such information include:

- reporting guidelines and contact information for RoCSIRT;
- archive or alerts, warnings and other announcements;
- documentation about best current practices;
- policies, procedures and checklist;
- vendor links;
- other information that can improve overall security practices.

6.3. Security Quality Management Services

These services leverage the CSIRT's expertise and focus on long-term issues.

6.3.1. Awareness Building

RoCSIRT will aim to increase security awareness among its constituents population through articles, newsletters, and any information source deemed necessary, in order to explain security best practices and provide advice on precautions to take. RoCSIRT can also schedule meetings and seminars to keep constituents up to date.

6.3.2. Education and Training

RoCSIRT will provide information about computer security issues through seminars; workshops, courses, or tutorials.

6.3.3. Advice to Legislative Bodies

Should the occasion arise, RoCSIRT would give testimonials or advice to legislative bodies.

7. Offline incident reporting form

When offline incident must be reported, please use the following Incident Reporting Form. An electronic version of the document will be found on RoCSIRT's web site. If the form is too complicated, the quick reporting electronic form (already available on the website) can be used in time critical situations.

version 2.0
November 2013
RoCSIRT
Incident Reporting Form

The following form has been developed to ease gathering incident information. If you believe you have been involved in an incident, please complete - as much as possible - the following form, and send it to team@csirt.ro . If you are unable to send email, please fax it to +40 021 3171174 . This information will be treated confidentially, as per our Information Disclosure Policy. This form is an adaptation of CSIRT/CC's incident reporting form, version 5.2.

RoCSIRT offline reporting form – English version

Your contact and organizational information

Name	
Organization name	
Connected to RoEduNet	
Email address	
Telephone number	
Fax number	
Other contact data	

Affected machine(s)

Hostname and IP addr	
Timestamp	
Timezone	
Services affected	

Source of the attack

Hostname and IP addr	
Timestamp	
Timezone	
Direct contact initiated	

Description of the incident

Dates	
Methods of intrusion	

Tools involved	
Software versions	
Intruder tool output	
Vulnerabilities exploited	
Other relevant information	

8. Disclaimer

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

9. Bibliography

[BG98] Neville Brownlee and Erik Guttman. RFC 2350, BCP21 – Expectations for Computer Security Incident Response. IETF, 1998.

[WBSK+ 03] Moira J. West-Brown, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle, and Mark Zajcek. Handbook for Computer Security Emergency Response Teams (CSIRTs). CMU/SEI, second edition, 2003.