
CSIRT Description for Pro-CERT

1. About this document.....	2
1.1 Date of Last Update	2
1.2 Distribution List for Notifications	2
1.3 Locations where this Document May Be Found.....	2
1.4 Authenticating this document	2
2. Contact Information.....	2
2.1 Name of the Team.....	2
2.2 Address	2
2.3 Timezone.....	2
2.4 Telephone Number.....	2
2.5 Facsimile Number	2
2.6 Other Telecommunication	2
2.7 Electronic Mail Address	2
2.8 Public keys and Other Encryption Information	3
2.9 Team Members	3
2.10 Other Information	3
2.11 Points of Customer Contact	3
3. Charter.....	3
3.1 Mission Statement.....	3
3.2 Constituency	3
3.3 Sponsorship and/or Affiliation.....	4
3.4 Authority	4
4. Policies.....	4
4.1 Types of Incidents and Level of Support.....	4
4.2 Co-operation, Interaction and Disclosure of Information.....	4
4.3 Communication and Authentication	5
5. Services.....	5
5.1 Incident Response	5
5.1.1 Incident Triage.....	5
5.1.2 Incident Coordination	5
5.1.3 Incident Resolution	5
5.2 Proactive Services.....	6
6. Incident Reporting Forms	6
7. Disclaimers	6

1. About this document

1.1 Date of Last Update

This is version 1.0.0, published on June 01, 2010

1.2 Distribution List for Notifications

Notifications of updates are submitted to our mailing list cert-announces@lists.pro-cert.ro. Archives for the list can be found at <http://lists.pro-cert.ro/mailman/private/cert-announces/>. Subscription information to the list is available at <http://lists.pro-cert.ro/mailman/listinfo/cert-announces/>

1.3 Locations where this Document May Be Found

The current version of this CSIRT description document is available from the Pro-CERT website <http://www.pro-cert.to/rfc2350.pdf>. Please make sure you are using the latest version.

1.4 Authenticating this document

The PDF version of this document has been signed with Pro-CERT PGP key. Given the difficulty in reliably signing web pages, the HTML versions are not digitally signed.

2. Contact Information

2.1 Name of the Team

"Pro CERT": Provision Romania Computer Emergency Response Team

2.2 Address

7 Fabrica de Glucoza, 2nd floor, district 3, Zip code 020331, Bucharest, Romania

2.3 Timezone

Eastern European Time (GMT+0200, GMT+0300 DST)

2.4 Telephone Number

+40 213 020 612 or +40 372 176 812

2.5 Facsimile Number

+40 372 176 812 (note this is not a secure fax)

2.6 Other Telecommunication

None available.

2.7 Electronic Mail Address

cert@pro-cert.ro This is a mail alias that serves the human(s) on duty for Pro CERT.

2.8 Public keys and Other Encryption Information

Pro CERT has a PGP key, which KeyID is 0xF9187E90 and which fingerprint is 4CD3 849E D3AF 2DA7 60BD A3E6 98DA 8B12 F918 7E90 The key and its signatures can be found at the usual large public key servers.

2.9 Team Members

Dragos LUNGU Pro CERT Coordinator
Eugeniu PATRASCU : Technical Director
Cornel ILIE : Analyst

2.10 Other Information

General information about Pro CERT , as well as links to various recommended security resources, can be found at <http://www.pro-cert.ro>

2.11 Points of Customer Contact

The preferred method for contacting Pro CERT is via e-mail at cert@pro-cert.ro ; e-mail sent to this address will be handled by the on-duty human analyst. We encourage our customers to use PGP encryption when sending any sensitive information to Pro CERT.

If e-mail is not possible, Pro CERT can be reached by telephone during regular office hours. Off these hours incoming phone calls are transmitted to an answering machine. All messages recorded are checked upon.

Pro CERT hours of operation are generally restricted to regular business hours (09:00 - 17:00 EET Monday to Friday except public holidays).

If possible, when submitting your incident report, use the form mentioned in section 6.

3. Charter

3.1 Mission Statement

Pro CERT offers assistance and coordination in early detection and handling of computer and network security incidents for all it's constituents. Pro CERT is dedicated to preventing security incidents by offering direct proactive measures and security quality management services.

3.2 Constituency

Pro CERT constituency include all networks and systems belonging to Provision Software Division SRL and it's customers.

3.3 Sponsorship and/or Affiliation

Pro CERT is a project initiated and sponsored by Provision Software Division SRL, the largest privately owned Romanian IT security company.

3.4 Authority

Pro CERT operates under the authority of Provision's Managed Security Services business division, which manages the operational authority between Pro CERT and each of its constituents through individual SLAs. Pro CERT has complete authority over AS25318 Autonomous System Number.

Pro CERT core activities imply close cooperation with all large ISP's abuse teams from Romania and abroad, direct contact and data exchange in order to prevent and recover from security incidents that affect Pro CERT's constituents.

All proactive services such as announcements and security related information dissemination are openly available to the public.

4. Policies

4.1 Types of Incidents and Level of Support

Pro CERT is authorized to address all types of computer security incidents which occur, or threaten to occur, in constituent networks.

The level of support given by Pro CERT will vary depending on the type and severity of the incident or issue, the type of constituent, the estimated impact and the Pro CERT's resources at the time, though in all cases some response will be made within two working days.

Incidents will be prioritized according to their apparent severity and extent.

End users are expected to contact their systems or network administrator. Only limited support can be given to end users.

4.2 Co-operation, Interaction and Disclosure of Information

Pro CERT exchanges all necessary information with other CSIRTs as well as with affected parties' representatives only after signing NDAs. No personal data is exchanged unless explicitly authorized.

All sensible data (such as personal data, system configurations, and known vulnerabilities with their locations) must be encrypted if needed to be transmitted over unsecured environment.

Pro CERT operates under the restrictions imposed by Romanian law. This involves careful handling of personal data as required by Romanian Data Protection laws, but it is

also possible that - according to Romanian law – Pro CERT may be forced to disclose information due to a Court's order.

4.3 Communication and Authentication

Given the nature of information that Pro CERT deals with, telephones will be considered sufficiently secure to be used even unencrypted. Unencrypted e-mail will not be considered particularly 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 will be used. Network file transfers will be considered to be similar to e-mail for these purposes: sensitive data should be encrypted for transmission.

All e-mail or data communication originating from Pro CERT will be digitally signed, using the generic PGP key mentioned above, or the Pro CERT team member's own signature keys.

5. Services

5.1 Incident Response

Pro CERT will assist anyone within the 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 management:

5.1.1 Incident Triage

- Investigating whether indeed an incident occurred.
- Determining the extent of the incident.

5.1.2 Incident Coordination

- Determining the initial cause of the incident. (which vulnerability was exploited)
- Facilitating contact with other sites which may be involved.
- Facilitating contact with appropriate law enforcement officials, if necessary.
- Making reports to other CSIRTs
- Composing announcements to public or constituents, if applicable

5.1.3 Incident Resolution

Pro CERT will provide incident resolution services for all constituents according to the mutually agreed SLAs. These services include :

- Providing assistance for removing the exploited vulnerabilities and enrolling in a complete vulnerability management system.

- Securing the systems from the effects of the incident and implementing security quality management services such as : Risk Analysis, Business Continuity / Disaster Recovery.
- Provide assistance in evidence collection and artifact analysis if required.

In addition, Pro CERT will collect statistics concerning incidents processed, and will notify the community as necessary to assist it in protecting against known attacks. To make use of Pro CERT's services please refer to section 2.11 for points of contact.

5.2 Proactive Services

One of the core goals of Pro CERT is stopping security incidents from happening through its extended range of proactive services. There are three pillars which make the foundation of Pro CERT's proactive services : people, technologies and processes.

The first component is represented by security training and educational services which are delivered in close partnership with Pro CERT's sponsor: Provision . For more details please see <http://www.securitytraining.ro/> for more details.

Another line of defense in Pro CERT's proactive services is made of state-of-the-art technologies deployed in the fields of : Intrusion Detection, SIEM (Security Information and Event Management), Configuration Monitoring and others.

Pro CERT's activity is regulated by well established policies and procedures which are derived from industry's best practices and it's worth mentioning that Pro CERT's sponsor, Provision has earned ISO 27001 Certification for Information Security Management.

6. Incident Reporting Forms

Pro CERT had created a local form designated for reporting incidents to the team. We strongly encourage anyone reporting an incident to fill it out, although this is never required. The current version of the form is available from:

<https://www.pro-cert.ro/form.php>

7. Disclaimers

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