

CSIRT

Description of RESTENA-CSIRT

1 About This Document

1.1 Version Information

Version 1.0, Date: 26 March 2008

1.2 Location Of This Document

The current version of this CSIRT description is available from the web site:

<http://www.restena.lu/csirt/>

1.3 Authentication Of This Document

The PDF version of this document has been digitally signed with the RESTENA-CSIRT PGP Key. The signature and the document are available on our web site at:

PDF File:

<http://www.restena.lu/restena/en/Pdfs/RESTENA-CSIRT-Description-v1.0.pdf>

Signature:

<http://www.restena.lu/restena/en/Pdfs/RESTENA-CSIRT-Description-v1.0.pdf.asc>

2 Contact Information

2.1 Name of the Team

RESTENA-CSIRT: RESTENA's Computer Security Incident Response Team

2.2 Address

Fondation RESTENA
RESTENA-CSIRT
6, rue Coudenhove-Kalergi
L-1359 Luxembourg
LUXEMBOURG

2.3 Timezone

Central European Time (GMT+0100), daylight saving time applies.

2.4 Telephone Number

+352.4244091 (office hours, Monday to Friday except holidays)

2.5 Fax Number

+352.422473 (this is *not* a secure fax)

2.6 Email

csirt@restena.lu

2.7 Team Members

- Gilles Massen
- Bruno Prémont
- Marc Stiefer
- Stefan Winter

Management and supervision are provided by Antoine Barthel and Theo Duhautpas, Directors of the RESTENA Foundation.

2.8 PGP Keys

2.8.1 CSIRT: csirt@restena.lu

This key is to be used for any confidential communication with RESTENA-CSIRT: communicating vulnerabilities, incidents, questions, as well as signing advisories and related information.

The public key can be found at the usual public key servers (such as: pgp-keys.pca.dfn.de).

PGP Key Id: 869540B2 <csirt@restena.lu> RESTENA-CSIRT

Fingerprint: 8574 F769 F66B BC28 2E43 2859 1B0D 4B7F 8695 40B2

2.8.2 Gilles Massen

PGP Key Id: D4BBD5A <gilles.massen@restena.lu>

Fingerprint: A184 AFB D B72E 3C68 B253 B3FD 6861 C769 4D4B BD5A

2.8.3 Bruno Prémont

PGP Key Id: 89CC5F56 <bruno.premont@restena.lu>

Fingerprint: EC35 8113 E00B F256 912B 00B9 7367 0ECB 89CC 5F56

2.8.4 Marc Stiefer

PGP Key Id: CFB050ED <marc.stiefer@restena.lu>

Fingerprint: CB0C CF77 56B9 2669 A105 F8DB 492E 26FB CFB0 50ED

2.8.5 Stefan Winter

PGP Key Id: FF1E1566 <stefan.winter@restena.lu>
Finderprint: 3881 E32C 18C4 E855 D593 E659 FA39 BDD1 FF1E 1566

2.9 Points of Contacts

The preferred method for contacting the CSIRT is via e-mail at *csirt@restena.lu*. If it is not possible (or not advisable for security reasons) to use e-mail, the CSIRT-team can be reached by telephone during regular office hours.

Please note that the RESTENA-CSIRT is not offering a 24-hours service. The hours of operation are generally restricted to regular business hours (08:00-16:45 Monday to Friday except holidays).

2.10 Other Information

General information about the RESTENA-CSIRT, as well as links to various recommended security resources, can be found at

<http://www.restena.lu/csirt/>

3 Charter

3.1 Mission Statement

The mission and goals are:

- support and coordinate security incident response within the constituency,
- serve as a trusted point of contact and act as clearing house for security incident-related information,
- improve awareness and knowledge of IT security among the constituents,
- keep contact with other CSIRT/ CERT teams and cooperate with national and international CERT organisations.

3.2 Constituency

RESTENA-CSIRT's constituency is the RESTENA Foundation's user community. This includes:

- University of Luxembourg
- Higher education institutions
- Public and private research centers
- Cultural institutions
- Primary and secondary schools
- Individual users

Individual users as well as small organisations with no or low technical knowledge will be handled through RESTENA Helpdesk and RESTENA NOC, which act as clients of the CSIRT on their own. Public services operated by RESTENA (like Internet Exchange (LIX) or .LU registry) are also CSIRT clients.

3.3 Sponsorship and Affiliation

The RESTENA-CSIRT is part of RESTENA's operations framework. It is operated and staffed by the RESTENA Foundation. RESTENA-CSIRT will establish affiliations with other CERT/CSIRT around Europe by seeking to become a TERENA TI accredited team, and maybe by an adhesion to FIRST.

3.4 Authority

RESTENA-CSIRT operates under the auspices of RESTENA Foundation. It expects to work cooperatively with the responsible staff of the institutions connected to the RESTENA network. The authority of RESTENA-CSIRT is established by the governing AUP.

4 RESTENA CSIRT Policy

4.1 Types Of Incidents And Level Of Support

The RESTENA-CSIRT is authorised to address all types of computer security incidents which occur, or threaten to occur, within its constituency.

The level of support given by RESTENA-CSIRT will vary depending on the type and severity of the incident or issue, the type of constituent and the RESTENA-CSIRT's resources available (on a best effort basis).

Note that no direct support will be given to end users. They are expected to contact their system- or network administrator, and especially the organisation's security contact(s) for assistance.

4.2 Disclosure Of Information

As a generale rule, all site-specific and personal information is kept private and confidential and is not disclosed to third parties without the consent of the concerned site or person. The exchange of information (if required or necessary) is carried out in an anonymised way only.

RESTENA-CSIRT operates according to Luxembourg law and regulations. Therefore, RESTENA-CSIRT may be forced to disclose information to the authorities, pursuant to a Court Order.

4.3 Communication And Authentication

For normal communication not containing sensitive information, RESTENA-CSIRT will use conventional methods like unencrypted email or fax.

For secure communication, PGP-encrypted email or telephone will be used. If it is necessary to authenticate a person before communicating, this can be done either through existing webs of trust or by other methods like call-back, mail-back or even face-to-face meeting.

5 Services

RESTENA-CSIRT will coordinate security incident prevention, handling and response within its constituency.

5.1 Reactive Services

These services are offered in reaction to an occurring security incident involving the constituency, be it detected by RESTENA-CSIRT staff, constituency's staff or reported to the team by an other CSIRT or third party.

5.1.1 Incident Response

Incident Triage

- interpretation of incoming security incident reports, tracking and prioritizing them;
- determination of the extent or scope of the security incident.

Incident Coordination

- contact the involved organisation(s) to investigate the incident and take the appropriate steps;
- notification of other involved parties on a need-to-know basis, as per the information disclosure policy;
- facilitating contact with appropriate security teams and/or law enforcement officials if necessary;
- making reports to other CSIRTs;
- sending announcements to users (members of constituency), if applicable.

Incident Resolution

- RESTENA-CSIRT will not provide active security incident resolution service to its constituency.

5.2 Proactive Services

5.2.1 Awareness and Knowledge Building

Proactive services are focused on educational aspects:

- increase security awareness and knowledge among the constituents through articles, best practices, or any other information, in order to explain security best practices and provide advice on precautions to take,
- schedule meetings and seminars to keep the constituency up-to-date,
- collect statistics about incidents within the constituency.

6 Incident Reporting Form

The incident report to be accepted by the CSIRT should contain all necessary information as specified in incidents reporting guidelines. An appropriate form has been made available for this purpose.

An electronic version of the document can be found on RESTENA-CSIRT's web site:

<http://www.restena.lu/restena/en/Pdfs/CSIRTReportingForm.txt>

RESTENA CSIRT
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
csirt@restena.lu
If you are unable to send email, please fax it to
+352 42 24 73
This information will be treated confidentially, as per our Information Disclosure Policy.
This form is an adaptation of CERT/CC's incident reporting form, version 5.2.
Your contact and organisational information
1. name.....:
2. organisation name.....:
3. are you a RESTENA customer.:
3.a if no:
 sector type (such as banking, education, energy or public safety).....:
4. email address.....:
5. telephone number.....:
6. other (fax, ...).....:
Affected Machine(s)
(duplicate for each host)
7. hostname and IP.....:
8. timezone.....:
9. purpose or function of the host (please be as specific as possible).....:
Source(s) of the Attack
(duplicate for each host)
10. hostname or IP.....:
11. timezone.....:
12. been in contact?.....:
Description of the incident (duplicate in case of multiple incidents)
13. dates.....:
14. methods of intrusion.....:
15. Tools involved.....:
16. Software versions.....:
17. Intruder tool output
18. Vulnerabilities exploited
19. Other relevant information

7 Disclaimer

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