RFC2350_NCERT (Public)

Version 1.0 - 2017.10.16 (Final)

Policy (POL 220)

TLP: TLP:WHITE

Classification: PUBLIC

Department: NCERT.LU

NCERT.lu | CERT national Luxembourg

Contents

Bureaux: 50, rue du Château
L-6961 Senningen
Adresse postale: B.P. 11
L-6905 Niederanven
Secrétariat: (+352) 247-88966
Téléfax: (+352) 247-88964
http://www.ncert.lu
info@ncert.lu

1 Introduction

1.1 Overview

This document is composed of several sections describing how works NCERT.LU. Each section gives guidelines and procedures permitting to a constituent to report, in a good manner, a security incident.

1.2 Purpose

This document contains a description of NCERT.LU according to *RFC 2350*. It provides information about the computer security incident response team (CSIRT), how to contact the team, and describes its responsibilities and the services offered by NCERT.LU.

1.3 Scope

This policy covers NCERT.LU constituency.

1.4 References

1. *FRM702.301 - Incident Reporting Form*
2. *POL202 - RFC2350*
3. *RFC 2350: Expectations for Computer Security Incident Response*. URL: https://www.ietf.org/rfc/rfc2350.txt

1.5 Definitions and Abbreviations

Abbreviation	Definition
PGP	Pretty Good Privacy
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team

Table 1: Definitions and Abbreviations

Bureaux: 50, rue du Château
L-6961 Senningen
Adresse postale: B.P. 11
L-6905 Niederanven
Secrétariat: (+352) 247-88966
Téléfax: (+352) 247-88964
http://www.ncert.lu
info@ncert.lu

2 Document Information

2.1 Date of Last Update

This is version 1.0, published on 2017.10.16.

This version is valid until superseded by a later version.

2.2 Distribution List for Notifications

Changes to this document are not distributed by a mailing-list, RSS or any other mechanism. Please address any specific questions or remarks to NCERT.LU e-mail address (see paragraph 3.7).

2.3 Locations Where This Document May be Found

The current version of this document is always available on NCERT.LU website at http://www.ncert.lu.

2.4 Authenticating This Document

This document has been signed with the PGP key of GOVCERT.LU.

The signature is available on web site http://www.govcert.lu.

3 Contact Information

3.1 Name of the Team

National CERT Luxembourg.

Short name: NCERT.LU.

3.2 Address

Ministère d'État - CERT National (NCERT.LU)
50, rue du Château
L-6961 Senningen
Grand Duchy of Luxembourg

3.3 Time Zone

CET / CEST

- GMT+01:00 in winter time (from last Sunday in October to last Sunday in March)
- GMT+02:00 during summer time (from last Sunday in March to last Sunday in October)

Bureaux: 50, rue du Château
L-6961 Senningen
TLP: TLP:WHITE

Adresse postale: B.P. 11
L-6905 Niederanven

Secrétariat: (+352) 247-88966
Téléfax: (+352) 247-88964

http://www.ncert.lu
info@ncert.lu
Classification: PUBLIC

3.4 Telephone Number

Secretariat: (+352) 247-88966

Hotline: (+352) 247-88960 (it doesn't cover totally the range of outside business hours. The principle of best effort is applied)

3.5 Facsimile Number

(+352) 247-88964 (this is *not* a secure fax)

3.6 Other Telecommunication

Internet Website: http://www.ncert.lu.

3.7 Email Address

info@ncert.lu: this e-mail address is used for exchanging general information. The reporting of incidents (see below) using this email address should be avoided.

soc@ncert.lu: this e-mail address is used for reporting an incident to the Support and Operation Center team of NCERT.LU.

3.8 Public Keys and Encryption Information

E-mail addresses (info@ncert.lu and soc@ncert.lu) used by NCERT.LU share the same PGP key, as documented below:

- Key Id: 0xE8B75E31
    - o Key Type: RSA-4096
    - o Key Fingerprint: A5AB0383 CF4138C5 0B5DF49D CC4A5C05 E8B75E31

The public key and its signatures can be found on the usual large public key servers as well as on NCERT.LU public web site (http://www.ncert.lu).

This key signs any communication from NCERT.LU. It is also used for any confidential communication with NCERT.LU (incident reports, alerts).

3.9 Team Members

NCERT.LU is operated by the Governmental CERT of Luxembourg. The staff consists of dedicated IT security experts from the State Ministry. The full list of NCERT.LU team members is not publicly available. Team members will identify themselves to the reporting party with their full name in an official communication regarding an incident.

3.10 Other Information

General information about NCERT.LU, as well as links to various recommended security resources, can be found on NCERT.LU public web site (http://www.ncert.lu).

Bureaux: 50, rue du Château
L-6961 Senningen
Adresse postale: B.P. 11
L-6905 Niederanven
Secrétariat: (+352) 247-88966
Téléfax: (+352) 247-88964
http://www.ncert.lu
info@ncert.lu

3.11 Points of Customer Contact

Days/hours of operation are 08:00 to 12:00 / 13:00 to 17:00 CET / CEST from Monday to Friday except during Luxembourg's public holidays.

All incidents reports should be sent to soc@ncert.lu. This e-mail address is preferred for reporting urgent, sensitive or critical information, information security events and incidents.

On a general manner, use of phone and fax for reporting incidents should be avoided as much as possible.

NCERT.LU encourages its constituents to use secure e-mail (for instance PGP) when exchanging any sensitive information.

4 Charter

4.1 Mission Statement

NCERT.LU acts at national and international level:

- to protect the Grand-duchy of Luxembourg against major cyber threats,
- to provide an attractive, secure and reliable environment for local businesses in Luxembourg,
- to protect Luxembourg's citizen's privacy and fundamental rights.

To fulfil its missions, NCERT.LU is mandated:

- to operate the official, national point of contact for foreign national and governmental CERTs,
- to operate as the official, national point of contact for the collection and distribution of information linked to security incidents that concern information systems implanted in Luxembourg,
- to be the interlocutor for physical and moral persons, on a national and international level,
- to convey incidents to the CERTs in charge of the affected victim's sector or, if no sectoral CERT exists, directly to the victim,
- to advise about the specific points of contact according to the targeted sector.

4.2 Constituency

The Constituency of NCERT.LU is made of any information systems implanted in Luxembourg.

4.3 Sponsorship and/or Affiliation

NCERT.LU is sponsored by the following entities in Luxembourg:

- HCPN: Haut-Commissariat à la Protection Nationale
- ANSSI: Agence Nationale de la Sécurité des Systèmes d'Information
- GOVCERT: CERT gouvernemental
- CTIE: Centre des Technologies de l'Information de l'Etat

Bureaux: 50, rue du Château
L-6961 Senningen
Adresse postale: B.P. 11
L-6905 Niederanven
Secrétariat: (+352) 247-88966
Téléfax: (+352) 247-88964
http://www.ncert.lu
info@ncert.lu

4.4 Authority

By way of Grand-Ducal decree, GOVCERT has been mandated to act as the official national point of contact for national and international governmental CERTs. It performs this function under the name of NCERT.LU (National CERT). NCERT.LU gathers and disseminates information about security incidents, which affect information and communication systems in Luxembourg. It also serves as interlocutor for natural and legal persons, entities and bodies, both national and international.

Once it has received information, NCERT.LU must convey it to the CERTs in charge of the affected victim's sector or, if no sectoral CERT exists, directly to the victim. NCERT.LU will also advise about the specific points of contact according to the targeted sector.

Constituents have to report information security incidents to NCERT.LU, and also have to provide contact information with regards to information security incidents.

All members of NCERT.LU team have necessary security clearances. As a consequence, they have wide possibilities of interacting with systems, services and system administrators from the constituency of NCERT.LU.

NCERT.LU operates within the confines imposed by Luxembourg's legislation.

5 Policies

Since NCERT.LU is operated by the governmental CERT the policies used at NCERT.LU are the same that are used by GOVCERT.LU

5.1 Types of Incidents and Level of Support

This part is covered by GOVCERT.LU Policy *POL202 - RFC2350*
The *POL202 - RFC2350* applicable to GOVCERT.LU can be found at http://www.govcert.lu.

5.2 Co-operation, Interaction and Disclosure of Information

This part is covered by GOVCERT.LU Policy *POL202 - RFC2350*
The *POL202 - RFC2350* applicable to GOVCERT.LU can be found at http://www.govcert.lu.

5.3 Communication and Authentication

The preferred method of communication is via e-mail. If it is not possible (or not advisable for security reasons) to use electronic communication (e-mail / web form), NCERT.LU can be reached by telephone during time of operation. Off these hours a Hotline phone is available but it doesn't cover totally the range of outside business hours. The principle of best effort is applied.

In view of the types of information that NCERT.LU deals with, telephones may 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 unclassified / low-sensitivity data.

Where it is necessary to establish trust, for example before relying on information given to NCERT.LU, or before disclosing confidential information, the identity and bona fide of the other party will be ascertained to

Bureaux: 50, rue du Château
L-6961 Senningen
Adresse postale: B.P. 11
L-6905 Niederanven
Secrétariat: (+352) 247-88966
Téléfax: (+352) 247-88964
http://www.ncert.lu
info@ncert.lu

a reasonable degree of trust. Within the constituency, and with known neighbour 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 is supported by NCERT.LU).

Communication security (encryption and authentication) is achieved by various means: PGP or other agreed means, depending on the sensitivity level and context.

If it is necessary to send highly sensitive data by e-mail, encryption (for instance 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. In such situation, all sensitive communication to NCERT.LU should be encrypted against the team's PGP key.

All e-mail or data communication related to an incident originating from NCERT.LU are digitally signed using PGP keys mentioned above, or NCERT.LU agents' own signature keys.

Use of encryption / digital signature is encouraged when reporting information to NCERT.LU, especially when sending sensitive information.

When submitting a report, (1) provide the operator with notice on the urgency along with the report, (2) your need for feedback, and (3) use where possible the form *FRM702.301 - Incident Reporting Form* available on http://www.govcert.lu.

6 Services

This part is covered by GOVCERT.LU Policy *POL202 - RFC2350*
The *POL202 - RFC2350* applicable to GOVCERT.LU can be found at http://www.govcert.lu.

6.1 Incident Response

This part is covered by GOVCERT.LU Policy *POL202 - RFC2350*
The *POL202 - RFC2350* applicable to GOVCERT.LU can be found at http://www.govcert.lu.

7 Disclaimer

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

Bureaux: 50, rue du Château
L-6961 Senningen
TLP: TLP:WHITE

Adresse postale: B.P. 11
L-6905 Niederanven

Secrétariat: (+352) 247-88966
Téléfax: (+352) 247-88964

http://www.ncert.lu
info@ncert.lu
Classification: PUBLIC