THE GOVERNMENT
OF THE GRAND DUCHY OF LUXEMBOURG
High Commission for National Protection

Governmental CERT

Responsible Disclosure Policy (Public)

Version 3.0 - 2024-08-29 (Final)

Policy (POL 226)

TLP: **TLP:CLEAR**

Contents

46, rue du Château
L-6961 Senningen
Secretariat: (+352) 247-88966
https://www.govcert.lu

1 Introduction

1.1 Overview

GOVCERT.LU is the single point of contact to obtain and process vulnerability informations for all systems owned by its constituency[1]. GOVCERT.LU provides the means to disclose the information in a responsible manner to any third party discovering such a vulnerability.

1.2 Purpose

This policy defines the guidelines on responsible disclosure of vulnerabilities to GOVCERT.LU by a third party.

1.3 Scope

The policy covers all vulnerabilities disclosed by a third party to GOVCERT.LU.

1.4 Definitions and Abbreviations

1.4.1 Abbreviations

Abbreviation	Definition
CERT	Computer Emergency Response Team
PGP	Pretty Good Privacy

Table 1: Definitions and Abbreviations

[1] https://www.govcert.lu/en/constituency/

46, rue du Château
L-6961 Senningen
Secretariat: (+352) 247-88966
https://www.govcert.lu

2 What to report to GOVCERT.LU

Security vulnerabilities[2] in software or hardware that could lead to severe operational disruptions, compromise the confidentiality, availability, or integrity of a resource.

3 Vulnerability reporting policy

GOVCERT.LU, at its discretion, reserves the right to accept or reject any disclosed vulnerability, based on the following guidelines:

- Handling of the potentially sensitive information prior to disclosure:
  - The vulnerability should **NOT** be disclosed publicly
  - The vulnerability should be reported as soon as possible after its discovery
- After reporting the vulnerability to GOVCERT.LU no information should be shared with others until the incident has been processed and resolved. Otherwise the report may be removed from the GOVCERT.LU Hall of Fame.
- The vulnerability must be unknown and severe enough to be considered as eligible for a mention in the Hall of Fame of GOVCERT.LU
- Vulnerabilities that have been reported previously are rejected.

If all conditions are met, GOVCERT.LU will notify the affected party. Once the vulnerability has been fixed or the 90-day grace period has expired, the reporter can choose to be recognised in the GOVCERT.LU Hall of Fame[3]. The 90-day grace period starts on the day the vulnerability is reported.

4 Vulnerability reporting instructions

- E-mail the report to soc@govcert.etat.lu.
- Encrypt the email using the PGP key available on GOVCERT.LU website.
- Provide as much information as possible to allow an efficient handling.

Contact details *(email address or telephone number)* must be valid in order to allow GOVCERT.LU to request additional information if required.

[2] https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/vulnerabilities-and-exploits

[3] https://www.govcert.lu/en/hall_of_fame/

46, rue du Château
L-6961 Senningen
Secretariat: (+352) 247-88966
https://www.govcert.lu