GOVCERT.lu

Responsible Disclosure Policy (Public)

Version 1.0 - 2019-12-02 (Final)

Policy (POL 226)

TLP:	TLP:WHITE	**Department:**	GOVCERT.LU
Classification:	PUBLIC		

Contents

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. 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

2 What to report to GOVCERT.LU

Vulnerabilities which occur in software or hardware of national institutions, agencies or bodies and may have an impact on security.

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 notifies the impacted party. Once the issue is resolved or after expiration of the grace period of 90 days after the initial report, the reporter may be mentioned (at his own discretion) in the Hall of Fame of GOVCERT.LU (this page) with a short description of the type of vulnerability 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.

Provided contact details (email address or telephone number) must be valid to allow GOVCERT.LU to contact the reporter in case more information is required.