Incident Reporting Guidelines for Constituents (Public)

Version 5.0 - 2020-07-21 (Final)

Procedure (PRO 301)

TLP: TLP:WHITE

Classification: PUBLIC

Department: GOVCERT.LU

Contents

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

1 Introduction

1.1 Overview

The response to an incident is dependent on the quality of the information reported by the constituent, on the reporting time frame and on the capacity of the organisation in charge of the incident to solve the problem. This procedure defines a reporting method to help the constituent to report an incident to GOVCERT.LU within the required time frame and a common set of terms between GOVCERT.LU and its constituency.

1.2 Purpose

The aim of this procedure is to define guidelines for reporting an incident.

1.3 Scope

This procedure concerns GOVCERT.LU members and its constituency.

1.4 References

1. *FRM702.301 - Incident Reporting Form*
2. *POL204 - Information Disclosure Policy*

1.5 Abbreviations

Abbreviation	Definition
CERT	Computer Emergency Response Team
CVE	Common Vulnerabilities and Exposures
DNS	Domain Name System
GOVCERT.LU	Governmental CERT of Luxembourg
ICMP	Internet Control Message Protocol
IDS	Intrusion detection system
IP	Internet protocol
RDP	Remote Desktop Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
VNC	Virtual Network Computing
WPAD	Web Proxy Auto-Discovery Protocol

Table 1: Definitions and Abbreviations

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

2 Definition

2.1 Event

An event is an occurrence or change of a particular set of circumstances:

NOTE 1: An event can be one or more occurrences, and can have several causes.

NOTE 2: An event can consist of something not happening.

NOTE 3: An event can sometimes be referred to as an 'incident' or 'accident'.

2.2 Information Security Incident (or Incident)

An information security incident (or incident) is a single or a series of unwanted or unexpected information security events (section 2.3) that have a significant probability of compromising business operations and threatening information security[1].

2.3 Information Security Event

An information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.

2.4 Critical System

A critical system is a system, an application, data or other resources that is essential to the survival of an organisation. When a critical system fails or is interrupted, core operations are significantly impacted.

2.5 Non Critical System

Non critical system is a system, an application, data or other resources which do not have strong impacts to the good operation of a constituent if compromised.

[1] where *information security* means preservation of confidentiality, integrity and availability of information

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

3 Incident Reporting Guidelines

Incident reports should include a description of the incident or event, using the appropriate taxonomy, and as much of the following information as possible; however, **reporting should not be delayed in order to gain additional information**:

- Constituent name
- Point of contact information including name, telephone, and email address
- Incident Category (see full list in table 3)
- Incident date and time, including time zone
- Location and name of all systems involved in the incident
- Method used to identify the incident (e.g. IDS[2], audit log analysis, system administrator)
- Actions[3] done (date, time, result)
- Impact
- Resolution
- Criticality of the system (e.g. national or local system, classified system, etc.)

Constituents should use this model when reporting incidents to GOVCERT.LU. Depending on the criticality of the incident, it is not always feasible to gather all the information prior to reporting. In that case, a constituent should continue to report information as it is collected.

To help a constituent to report an incident to GOVCERT.LU, a reporting form is available on the website of GOVCERT.LU (https://www.govcert.lu).

After having filled out the reporting form, a constituent sends it within the required time frame (see table 3) by email to address: soc@govcert.etat.lu. The emails should be encrypted if possible or needed. The anonymous form can be used to report incidents anonymously but one should know that if no contact details are provided in the report, GOVCERT.LU will not respond to the report.

For general questions except for reporting incidents, you can also write directly to email address info@govcert.etat.lu or call our Hotline ((+352) 247-88960).

4 Incident Reporting Time Frame

The incident reporting time frames defined table 3 correspond to time frames in which constituents shall report the incident. Once these time frames are exceeded, GOVCERT.LU cannot ensure that an incident will be solved efficiently.

[2] Intrusion detection system

[3] **In order to preserve the evidence and keep investigation capacity for GOVCERT.LU, actions done for containing the incident shall be limited to the strict minimum (no re-installation of the operating system or of any software).**

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

5 Service Level Agreement (SLA)

Once an incident has been recorded by GOVCERT.LU, a notification email is automatically sent to the requestor. This email informs the requestor that the incident has been registered by GOVCERT.LU and provides a unique incident tracking number which shall be used for every communication with GOVCERT.LU concerning that specific incident.

Once the incident is registered, GOVCERT.LU starts the incident identification phase (incident category and priority allocation). This phase is followed by the incident response phase which consists in resolving the incident.

Depending on the incident priority, GOVCERT.LU agrees to meet the following SLA **for starting** the incident response phase (threat containment and eradication, recovery of the targeted information or system):

Levels	Maximum time frame for starting incident response phase[4]
Priority 1	24h after the incident registering
Priority 2	16h after the incident registering
Priority 3	8h after the incident registering
Priority 4	4h after the incident registering

Table 2: Priority Levels

6 Incident Categories

In order to clearly communicate incidents and events (any observable occurrence in a network or system) throughout the supported organisations, it is necessary for GOVCERT.LU and its constituency to adopt a common set of terms and relationships between those terms.

Below is a high level set of concepts and descriptions to categorise information security incidents:

The reading order of table 3 is top to bottom and the first category which matches with the incident is chosen (first match basis).

[4] Business hours.

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

Name & Description	Reporting Time Frame After Discovery	
	Critical system	Non critical system
1 - Information Content Security Unauthorised access to information, modification of information or loss of data: - by abusing stolen login credentials for a system or application - intercepting traffic - gaining access to physical documents - a ransomware encrypting data - loss of data caused by hard disk failure or physical theft	Within 1 hour.	Within 4 hours.
2 - Intrusions Compromise of a system or an application where the attacker: - gained administrative privileges - using an unprivileged (user/service) account - by exploiting (un-)known software vulnerabilities, e.g. SQL[5] injection Physical intrusion, e.g. into corporate building or data-centre.	Within 1 hour.	Within 1 hour.
3 - Malicious Code System infected with malware, e.g. PC, smartphone or server infected with a rootkit or which contacted a command-and-control (C2) server. URI used for malware distribution or malware configuration, e.g. a URL included in fake invoice or web-injects for a banking trojan.	Within 1 hour if widespread across organisation otherwise 1 day.	Within 4 hours if widespread across organisation otherwise 1 day.
4 - Availability Denial of Service attack, e.g. sending specially crafted requests to a web application which causes the application to crash or slow down, SYN-Floods or UDP-based reflection attacks. Physical sabotage or outage, e.g cutting wires or malicious arson or caused by air condition failure or natural disaster.	Within 2 hours if the successful attack is still ongoing and the organisation is unable to successfully mitigate activity.	Within 4 hours if the successful attack is still ongoing and the organisation is unable to successfully mitigate activity.
5 - Fraud - Using resources for unauthorised purposes including profit-making ventures. - Offering or installing copies of unlicensed commercial software or other copyright protected materials (Warez). - Impersonation of the identity of another in order to benefit from it. - Masquerading as another entity in order to persuade the user to reveal private credentials (phishing).	Within 4 hours.	Within 1 day.
6 - Abusive Content - SPAM, IoC's referring to resources, which make up a SPAM infrastructure, be it a harvesters like address verification, URLs in spam e-mails etc. - Discrimination of somebody - Child Sexual Exploitation, Sexual content, glorification of violence, etc.	Within 4 hours.	Within 1 day.

[5] Structured Query Language

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

Name & Description	Reporting Time Frame After Discovery	
	Critical system	Non critical system
7 - Information Gathering - Attacks that send requests to a system to discover weaknesses. e.g. fingerd, DNS[6] querying, ICMP[7], SMTP[8], port scanning. - Observing and recording of network traffic (wiretapping). - Gathering information from a human being in a non-technical way (e.g. lies, tricks, bribes, or threats).	Within 1 hour.	Within 2 weeks.
8 - Intrusion Attempts - An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardised identifier such as CVE[9] name (e.g. buffer overflow, backdoor, cross site scripting, etc.) - Multiple login attempts (Guessing / cracking of passwords, brute force). - An attack using an unknown exploit.	Within 1 hour.	Within 2 weeks.
9 - Vulnerable - Publicly accessible services offering weak crypto (e.g. web servers susceptible to POODLE/FREAK attacks). - Publicly accessible services that can be abused for conducting DDoS reflection/amplification attacks (e.g. open DNS resolvers). - Potentially unwanted publicly accessible services (e.g. Telnet, RDP[10] or VNC[11]). - Publicly accessible services potentially disclosing sensitive information (e.g. SNMP[12] or Redis). - A system which is vulnerable to certain attacks. Example: misconfigured client proxy settings (e.g. WPAD[13], outdated operating system version, etc.).	Within 6 hours.	Within 1 week.
10 - Other All incidents which do not fit in one of the given categories should be put into this class or the incident is not categorised.	Within 6 hours.	Within 1 day.
11 - Test Meant for testing.	Not applicable.	Not applicable.

Table 3: Information Security Incident Categories

[6] Domain Name System
[7] Internet Control Message Protocol
[8] Simple Mail Transfer Protocol
[9] Common Vulnerabilities and Exposures
[10] Remote Desktop Protocol
[11] Virtual Network Computing
[12] Simple Network Management Protocol
[13] Web Proxy Auto-Discovery Protocol

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

7 Disclosure Policy

All information addressed to GOVCERT.LU is processed in accordance with the *POL204 - Information Disclosure Policy* available on https://www.govcert.lu.

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

8 Appendix

List of documents created for this procedure	
FRM702.301	Incident Reporting Form (.DOCX and .TXT)

Table 4: List of the Documents Created for this Procedure

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