malware.lu CERT

Vulnerability disclosure

General information

Type	Policy
Sequence number	C100
Version	1.2
State	Final
Approved by	C. Harpes
Date	27/02/2017
Classification	Public

Document history

Version	Date	Modifications
0.1	28/03/2014	Document creation.
1.0	02/04/2014	Document approval.
1.1	15/05/2014	Adaptation ch. 1.2.1 on contacting vendors.
1.2	27/02/2017	Validation

Distribution list

Changes to this document are not distributed by a mailing list, RSS or any other mechanism. Please address any specific questions or remarks to malware.lu CERT e-mail address cert@malware.lu.

Working group

Name	Organisation
T. Mouelhi, N. Kasselouris, C. Muller, C. Harpes	itrust consulting

Approbations

Name	Role	Responsibility	Date	Signature
N. Kasselouris	Head of ethical hacking	Content agreement	27/02/2017	See printed version managed by CISO.
C. Muller	CISO	Quality agreement	27/02/2017	See printed version managed by CISO.
C. Harpes	Managing Director	Applicability	27/02/2017	See printed version managed by CISO.

Locations where this document may be found

The current version of the vulnerability disclosure policy is available on the malware.lu web site: http://www.malware.lu.

Table of contents

1 Introduction

1.1 Context

This policy is meant to define the rules followed by malware.lu CERT regarding vulnerability disclosure. It aims specifically at ensuring security for malware.lu CERT constituency and at enabling vendors to develop solutions for their security problems.

1.2 Objectives

The objectives of this policy are to define how vulnerabilities are disclosed and which rules to apply for contacting vendors affected by the vulnerabilities.

1.3 Document structure

The chapters of this report are structured as follows:

- Chapter 2 outlines the rules to be applied when disclosing vulnerabilities, including how to contact vendors and the publication schedule.

1.4 References

[1] STA_C003_CSIRT organisational chart.

1.5 Glossary

Terminology	Description
Computer security incident response team (CSIRT)	Team of appropriately skilled and trusted members of the organisation that handles information security incidents during their lifecycle.
Information security event	Occurrence indicating a possible breach of information security policies or failure of controls.
Information security incident	One or multiple related and identified information security events that may harm an organisation's assets and/or compromise its operations.
Information security incident management	Exercise of a consistent and effective approach to the handling of information security incidents.
Incident handling	Actions of detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents.
Incident response	Actions taken to protect and restore the normal operational conditions of an information system and the information stored in it when an information security incident occurs.

1.6 Acronyms

Acronym	Definition
CERT	Computer Emergency Response Team.
CSIRT	Computer Security Incident Response Team.

2 malware.lu CERT vulnerability disclosure policy

2.1 Vulnerability disclosure rules

Vulnerabilities are only disclosed after approval by the Managing Director of itrust consulting s.à r.l. and the CSIRT Manager of malware.lu CERT (see [1]).

2.1.1 Contacting vendors

malware.lu CERT coordinates all reported or detected vulnerabilities with the affected vendors.

malware.lu CERT negotiates the publication schedule with the affected vendors before publishing any vulnerability. If the vendor is unresponsive or mutual understanding on the disclosure schedule cannot be achieved, information about the vulnerabilities should be sent to a coordinating CSIRT acting as a trusted intermediary between vulnerability discoverers and vendors. Information about vulnerabilities is made public after 45 days of the initial report if no progress is stated, regardless of the existence or availability of patches or workarounds from affected vendors.

Disclosures made by the malware.lu CERT includes credit to the reporter unless otherwise requested. Vulnerabilities reported to us will be forwarded to the affected vendors as soon as possible after the initial report. The identity of the reporter is disclosed to the affected vendors unless otherwise requested. We will advise the reporter of significant changes in the status of his report to the extent possible without revealing information provided to us in confidence by the vendor.

malware.lu CERT reserves the right to use trusted third parties such as other coordinators and CSIRTs to relay vulnerability information to vendors. malware.lu CERT may also inform trusted third parties prior to the publication of vulnerability information. Vendors will be kept up to date of information sharing partners to the extent possible.

2.1.2 Publication schedule

An appropriate timeframe for mitigation development and the type and schedule of disclosure will be determined based on factors including:

- Whether the vulnerability has already been publicly disclosed;
- The severity of the vulnerability;
- Potential impact to critical infrastructure;
- Possible threat to public health and safety;
- Immediate mitigations available;
- Vendor responsiveness and feasibility for creating an upgrade or patch;
- Vendor estimate of time required for customers to obtain, test and apply the patch.

The name and contact information of the reporter will be forwarded to the affected vendors unless otherwise requested by the reporter. malware.lu CERT will advise the reporter of significant changes in the status of any vulnerability reported to the extent possible without revealing information provided in confidence by the vendor.

It is the goal of this policy to balance the need of the control system community to be informed of security vulnerabilities with the vendors' need for time to respond effectively. The final determination of the type and schedule of publication will be based on the best interests of the community overall.