CSIRT
SERVICE DESCRIPTION
RFC 2350

Hacknowledge

Hacknowledge SA

Le Tresi 9
1028 Préverenges
SWITZERLAND

Hacknowledge Lux SA

9 Rue du Laboratoire
1911 Luxembourg
Luxembourg

CSIRT

SERVICE DESCRIPTION RFC 2350

Index

1. Introduction

This document contains a description of CSIRT Hacknowledge (HACKNOWLEDGE SA) as implemented by RFC 2350. It provides information about CSIRT (HACKNOWLEDGE SA), as channels of communication, roles, responsibilities, and the services offered.

1.1. Date of last update

Version 1, created on 2021-03-21

1.2. Distribution list for notifications

There is no distribution list for notifications. This document is kept up to date at the location specified in 1.3. Should you have any questions regarding updates, please contact the CSIRT (HACKNOWLEDGE SA) email address.

1.3. Locations where this document may be found

The current and latest version of this document is available from HACKNOWLEDGE's website from this URL: https://hacknowledge.com/incident-response/csirt-service-description.pdf

1.4. Authenticating this document

This document has been signed with the PGP key of CSIRT (HACKNOWLEDGE SA).

The signature is available from HACKNOWLEDGE's website, from this URL :

https://hacknowledge.com/incident-response/csirt-service-description.pdf.sig

1.5. Document identification

- Title: **CSIRT_HACKNOWLEDGE_SERVICE-DESCRIPTION_RFC-2350**
- Version: 1
- Document Date: 2021-03-21
- Expiration: This document is valid until superseded by a more recent version

2. Contact Information

This section describes how to contact CSIRT (HACKNOWLEDGE SA) for Switzerland and Luxembourg.

2.1. Name of the team

- Full name: HACKNOWLEDGE SA
- Short name: HACKNOWLEDGE

2.2. Address

Switzerland:

Hacknowledge SA
Le trési 9B
1028 Préverenges
Switzerland

Luxembourg:

Hacknowledge Lux SA
9 Rue du Laboratoire
1911 Luxembourg
Luxembourg

2.3. Time zone

GMT+1 (with Daylight Saving Time or Summertime, which starts on the last Sunday in March and ends on the last Sunday in October). Also known as CET/CEST.

2.4. Telephone number

Switzerland:

Tel: +41 21 519 05 01

Luxembourg:

Tel: +352 20 30 15 86

2.5. Facsimile number

None available

2.6. Electronic mail address

If you need to notify us about an information security incident, please contact us at:
csirt@hacknowledge.com

2.7. Public Keys and Encryption Information

PGP/GnuPG is supported to secure communication.

Consequently, the CSIRT (HACKNOWLEDGE SA) has a PGP key:

• KeyID: 2C7AAA59

• Fingerprint: 5433 7EBE 2FA9 11CD 02AD 50B0 D258 E06F 2C7A AA59

The PGP key is available from HACKNOWLEDGE's website, from this URL: https://hacknowledge.com/incident-response/csirt-pkey.asc

The key shall be used whenever information related to security incident, must be sent to CSIRT (HACKNOWLEDGE SA) in a secure manner.

• Please use this key to encrypt messages that you send to CSIRT (HACKNOWLEDGE SA).

• When required CSIRT (HACKNOWLEDGE SA) will sign messages.

• When required, sign your messages using your own key please. It helps when that key is verifiable (for instance, using the public key servers).

2.8. Team members

CSIRT (HACKNOWLEDGE SA) in charge team leader is Yoann CHEVALIER.

The team consists of IT security specialist with broad skills in defensive and offensive security.

2.9. Other information

General information about CSIRT (HACKNOWLEDGE SA) can be found at the following URL:

https://hacknowledge.com/incident-response/

2.10. Point of customer contact

The preferred method to contact CSIRT (HACKNOWLEDGE SA) is to send an email to the following address: csirt@hacknowledge.com

E-mails sent to this address will be automatically forwarded to the on-call person If you require urgent assistance, put "[URGENT]" in your subject line.

3. CHARTER

This section describes CSIRT (HACKNOWLEDGE SA)'s mandate.

3.1. Mission statement

CSIRT (HACKNOWLEDGE SA) is a private CSIRT team delivering security services, mainly in Switzerland and Luxembourg.

Its main purpose is to assist its customer community:

- First, in evaluating customer capacity to suffer a possible security breach and recover from it efficiently.
- Second, implementing proactive measures to reduce the risks of computer security incidents.
- And third, in responding to such incidents whenever they occur.

CSIRT (HACKNOWLEDGE SA)'s mission is to support its customer community to protect themselves against both

The scope of CSIRT (HACKNOWLEDGE SA) activities cover prevention, detection, response, and support on recovery.

CSIRT (HACKNOWLEDGE SA) oversees digital forensics and incident response (DFIR) activities.

CSIRT (HACKNOWLEDGE SA) are driven by several key values:

• CSIRT (HACKNOWLEDGE SA) strives to act according to the highest standards of ethics, integrity, honesty and professionalism.

• CSIRT (HACKNOWLEDGE SA) is committed to deliver a high-quality service to its constituency.

• CSIRT (HACKNOWLEDGE SA) will ensure to respond to security incidents as efficiently as possible.

• CSIRT (HACKNOWLEDGE SA) will ease the exchange of good practices between constituents and with peers, on a need-to-know basis.

3.2. Constituency

CSIRT (HACKNOWLEDGE SA)'s primary constituency is composed of all the elements of HACKNOWLEDGE SA Information system composed of:

- Users
- Systems
- Applications
- Networks

However, CSIRT (HACKNOWLEDGE SA)'s services are also delivered to a secondary

constituency.

As a commercial CSIRT, the CSIRT (HACKNOWLEDGE SA)'s also provides services to its customers base, who subscribed a "Incident Response" support contract.

Current customers which are in Switzerland or Luxembourg are found among:

• Private sector organizations

• Public sector bodies

• Commercial bodies

3.3. Sponsoring Organization / Affiliation

CSIRT (HACKNOWLEDGE SA) is a private CSIRT. It is owned and operated by HACKNOWLEDGE.

It maintains relationships with various CSIRTs in Switzerland and Luxembourg.

CSIRT (HACKNOWLEDGE SA) is officially member of FIRST since 19 December 2018.

https://www.first.org/members/teams/hacknowledge

3.4. Authority

CSIRT (HACKNOWLEDGE SA) coordinates security incidents on behalf of its constituency, and only at its constituents' request. Consequently, CSIRT (HACKNOWLEDGE SA) operates under the endorsement, guidance and authority delegated by its constituents.

CSIRT (HACKNOWLEDGE SA) primarily acts as an advisor regarding local security teams and is expected to make operational recommendations. Therefore, CSIRT (HACKNOWLEDGE SA) may not have any specific authority to require specific actions.

The implementation of such recommendations is not a responsibility of CSIRT (HACKNOWLEDGE SA), but solely of those to whom the recommendations were made.

4. POLICIES

4.1. Types of Incidents and Level of Support

CSIRT (HACKNOWLEDGE SA) addresses all types of computer security incidents (cyber-attacks) which occur, or threaten to occur, in its constituency (see 3.2).

The level of support given by CSIRT (HACKNOWLEDGE SA) will vary depending on the type and severity of the incident or issue, its potential or assessed impact, the type of constituent, the size of the user community affected, and CSIRT (HACKNOWLEDGE SA) 's resources at the time. Depending on the security incident's type, CSIRT (HACKNOWLEDGE SA) will gradually roll out its services which include incident response and digital forensics.

Note that no direct support will be given to end users. They are expected to contact their internal IT department. The CSIRT (HACKNOWLEDGE SA) will support the latter people.

4.2. Co-operation, Interaction and Disclosure of Information

CSIRT (HACKNOWLEDGE SA) considers the importance of operational coordination and information sharing between CERTs, CSIRTs, SOCs and similar bodies, and with other organizations, which may aid to deliver its services, or which provide benefits to CSIRT (HACKNOWLEDGE SA)'s constituency.

Consequently, CSIRT (HACKNOWLEDGE SA) exchanges all necessary information with affected parties, as well as with other CSIRTs, on a need-to-know basis.

However, neither personal nor overhead data are exchanged unless explicitly authorized. Moreover, CSIRT (HACKNOWLEDGE SA) will protect the privacy of its customers/constituents, and therefore (under normal circumstances) pass on information in an anonymized way only (unless other contractual agreements apply). All incoming information is handled confidentially by CSIRT (HACKNOWLEDGE SA), regardless of its priority.

All sensible data (such as personal data, system configurations, known vulnerabilities with their locations) are stored in a secure environment, and are encrypted if they must be transmitted over unsecured environment as stated below.

CSIRT (HACKNOWLEDGE SA) supports the Information Sharing Traffic Light Protocol version 1.1 (see https://www.trusted-introducer.org/ISTLPv11.pdf). Information that comes in with the tags WHITE, GREEN, AMBER or RED will be handled appropriately.

CSIRT (HACKNOWLEDGE SA) operates within the current Swiss and Luxembourgish legal framework.

4.3. Communication and Authentication

CSIRT (HACKNOWLEDGE SA) protects sensitive information in accordance with relevant Swiss and European regulations and policies within Swiss and the EU. CSIRT (HACKNOWLEDGE SA) respects the sensitivity markings allocated by originators of information communicated to CSIRT (HACKNOWLEDGE SA) ("originator control").

CSIRT (HACKNOWLEDGE SA) also recognizes and supports the FIRST TLP (Traffic Light Protocol) version 1.1.

Communication security (which includes both encryption and authentication) is achieved using PGP primarily or any other agreed means, depending on the sensitivity level and context.

In CSIRT (HACKNOWLEDGE SA) 's context of operations, the following communication security levels may be encountered:

• Telephones will be considered sufficiently secure to be used (even unencrypted), in view of the types of information that CSIRT (HACKNOWLEDGE SA) deals with.

• Unencrypted email will not be considered particularly secure but will be enough for the transmission of low sensitivity data.

• If it is necessary to send highly sensitive data by email, encryption (preferably PGP) will be used (See 2.7). Network file transfers will be like email for these purposes: sensitive data should be encrypted for transmission. Regarding our SOC's customers, file transfer using the "file sharing" functionality of our portal remains a possibility.

5. Services

This section describes CSIRT (HACKNOWLEDGE SA)'s services.

5.1. Announcements

CSIRT (HACKNOWLEDGE SA) may provide information on the threat landscape, published vulnerabilities, new attack tools or artefacts and security measures.

5.2. Alerts and Warnings

CSIRT (HACKNOWLEDGE SA) distribute information on cyberattacks, disruptions, security vulnerabilities, intrusion alerts, malware, and provides recommendations to tackle the issue within its constituency. Alerts and warnings may be passed on to other CERTs, CSIRTs, SOCs and similar bodies if deemed necessary or useful to them on a need-to-know basis.

CSIRT (HACKNOWLEDGE SA) is not responsible for the implementation of its recommendations. Incident resolution is usually left to the responsible administrators within the constituency. However, CSIRT (HACKNOWLEDGE SA) will offer support and advice on request.

5.3. Pre-emptive Security Controls

CSIRT (HACKNOWLEDGE SA) performs pre-emptive security controls to detect potential breaches or vulnerabilities and misconfigurations that may be leveraged in cyberattacks. The security controls also check the compliance level of various systems and applications with the security policies.
CSIRT (HACKNOWLEDGE SA) handles both the triage and coordination aspects. Incident resolution is left to the responsible administrators within the constituency. However, CSIRT (HACKNOWLEDGE SA) will offer support and advice on request.

5.4. Digital Forensics and Incident Response (Triage, Coordination and Resolution)

CSIRT (HACKNOWLEDGE SA) performs incident response for its constituency (as defined in 3.2).

CSIRT (HACKNOWLEDGE SA) handles both the triage and coordination aspects. Incident resolution is left to the responsible administrators within the constituency. However, CSIRT (HACKNOWLEDGE SA) will offer support and advice on request.

CSIRT (HACKNOWLEDGE SA) will assist IT Security team in handling the technical and organizational aspects of incidents. It will aid or advice with respect to the following aspects of incident management:

Incident Triage:

- Investigating whether indeed an incident occurred
- Determining the extent of the incident

Incident Coordination:

- Determining the initial cause of the incident (vulnerability exploited)
- Performing acquisition and Digital Forensics whenever necessary (including hard drive and memory forensics)
- Facilitating contact with Security Contacts and/or appropriate law enforcement officials, if necessary
- Making reports to other CSIRTs, CERTs, SOC (if applicable)

Incident Resolution:

- Providing guidance and support to fix the vulnerability
- Providing support in securing the system from the effects of the incident
- Evaluating whether certain actions are likely to reap results in proportion to their cost and risk
- Collecting evidence where criminal prosecution, or disciplinary action, is contemplated

5.5. Development of Security Tools

CSIRT (HACKNOWLEDGE SA) internally develops security tools for its own use, to improve its services and support its activities as needed.

6. Incident Reporting Forms

No local form has been developed to report incidents to CSIRT (HACKNOWLEDGE SA).

In case of emergency or crisis, please provide CSIRT (HACKNOWLEDGE SA) at least the following information:

- Contact details and organizational name, including address and telephone number.
- Date and time when the incident started.
- Date and time when the incident was detected.
- Incident description.
- Affected assets, impact.
- Actions taken so far.
- Expectations or priorities.