NATIONAL CYBER SECURITY UNIT
PRINCIPALITY OF LIECHTENSTEIN

CSIRT.LI

RFC 2350 (Public)

Version 1.0 – 2024-03-21

Contents

1. Document information

This document, following RFC 2350 (Expectations for Computer Security Incident Response[1]), provides a summary of basic information about the national CSIRT of the Principality of Liechtenstein. In particular contact options, who belongs to the constituency and how to notify about incidents, as well as information about its role and services are provided within this document.

1.1 Date of last update

The initial version 1.0 published on 2024-03-21 is valid until superseded by a later version.

1.2 Distribution list for notifications

Changes to this document are distributed by a mailing-list, for which interested constituents from Liechtenstein can register by sending an e-mail under their business e-mail-address with subject “Register to CSIRT.LI RFC2350 notifications” to team@csirt.li.

1.3 Access Points for this document

The current version of this document is available at https://www.csirt.li.

1.4 Authenticating this document

This document has been digitally signed by Peter Wohlgenannt, the Head of CSIRT.LI.

[1] https://www.ietf.org/rfc/rfc2350.txt

2. Contact information

2.1 Name of the team

Short Name: CSIRT.LI
Full Name: Computer Security Incident Response Team Liechtenstein

2.2 Address

National Cyber Security Unit – CSIRT.LI
Zollstrasse 45
P.O. Box 684
LI-9490 Vaduz

2.3 Time zone

We are located in the central European time zone (CET/CEST) which is GMT+0100 (+0200 during day-light saving time).

2.4 Telephone number

At office hours from 08:00 to 16:00 CET/CEST: +423 236 63 11

We may operate outside office hours and days in case of an emergency only.

2.5 Other telecommunication

N/A.

2.6 Electronic mail address

Non-incident related e-mail should be addressed to team@csirt.li.

For notifying CSIRT.LI about an incident, use our web form as the primary method. The link to the web form can be found under point 5.3. If it's not possible to use the web form, constituents can send the incident notification to report@csirt.li.

2.7 Public keys and encryption information

CSIRT.LI uses Pretty Good Privacy (PGP) as well as S/MIME to secure communication via the e-mail addresses report@csirt.li and team@csirt.li. The PGP public keys as well as the S/MIME-certificates can be found on the public website of CSIRT.LI, as well as on the OpenPGP-keyserver in case of PGP. The key and certificate details are documented below.

UID: team@csirt.li <team@csirt.li>
Key Type: <RSA-4096>
Key Fingerprint: 7B71 9450 7382 7F67 783E E599 7F8F 55C4 EA7F 4B0C
Locations:

- Contact section of https://www.csirt.li
- https://keys.openpgp.org/vks/v1/by-fingerprint/7B71945073827F67783EE5997F8F55C4EA7F4B0C

UID: report@csirt.li <report@csirt.li>
Key Type: <RSA-4096>
Key Fingerprint: B478 3E7B 1FB9 D84D 5D05 FFF2 068D 4715 B35A D45D
Locations:

- Contact section of https://www.csirt.li
- https://keys.openpgp.org/vks/v1/by-fingerprint/B4783E7B1FB9D84D5D05FFF2068D4715B35AD45D

The S/MIME root, intermediate and user certificates can be found on the contact section of https://www.csirt.li.

2.8 Team members

The Head of CSIRT.LI is Peter Wohlgenannt. CSIRT.LI has dedicated team members.

2.9 Other information

According to the Liechtenstein implementation of the EU NIS Directive CSIRT.LI is the national CSIRT since July 2023 by law.

2.10 Points of customer contact

The preferred method to get in touch with CSIRT.LI is via e-mail team@csirt.li. Incident notifications should be submitted via our web form (link provided under point 5.3) to fall under the procedures of the Cyber Security Law. If this is not possible for whatever reason, the e-mail address report@csirt.li should be used for submission. The message should contain the information specified in the web form[2][3] and should be in plain text. Only notifications from registered constituents will be processed, see point 3.2.

[2](en) https://www.llv.li/serviceportal2/amtsstellen/stabstelle-cyber-sicherheit/notification_form_cyber_v1_0.pdf
[3](de) https://www.llv.li/serviceportal2/amtsstellen/stabstelle-cyber-sicherheit/formular_meldung_cyber_v1_0-1-.pdf

3. Charter

3.1 Mission statement

In the role of a national CSIRT within the NIS framework, the CSIRT.LI acts as the international point of contact (PoC) and functions as the national cyber security incident response coordinator.

CSIRT.LI mainly understands itself as a hub, primarily focused on efficiently directing information to the right places for aiding in the swift and effective resolution of IT security incidents. Our role is to facilitate communication and action, ensuring that critical data reaches the necessary experts and teams who can address and resolve these security challenges. By acting as a central point for information exchange, we help streamline the process of managing IT security incidents, making it easier for all involved parties to collaborate towards a timely and successful cleanup.

Furthermore, we also notify the public about concrete security incidents when raising awareness is deemed crucial for the prevention of further incidents or for the management of current ones.

3.2 Constituency

The constituency of CSIRT.LI is defined in Art. 1 Cyber Security Law (CSG) of 4 May 2023[4] and consists of operators of essential services (critical infrastructure) and providers of digital services (in the NIS-context) that are essential for the Liechtenstein citizens.

Note that no direct technical support will be given to end users; they are expected to contact their ISP, system administrator, network administrator or department head for assistance. CSIRT.LI will support the latter if required.

3.3 Sponsorship and/or affiliation

CSIRT.LI is fully sponsored by the government of Liechtenstein and is a department of the National Cyber Security Unit (SCS), which itself belongs to the Ministry of General Government Affairs and Finance led by the Prime Minister of Liechtenstein.

3.4 Authority

The authority is described in the law and corresponding regulations. According to Art. 5, 7 and 8 of the CSG constituents have to notify about information security incidents that significantly impacts the availability of a service they provide in the European Economic Area (EEA) to CSIRT.LI.

A notification about a security incident may serve as the basis for the creation of a situation report, a warning or an alert mentioned under 3.1, on which the stakeholders can protect themselves against similar attacks by reviewing and if necessary adapting their security measures (notification from affected constituent -> analysis -> situation report/warning/alert -> preventive measures taken by other constituents or partners). Note that a notification is not a trigger for the CSIRT to act beyond the analysis, assessment and processing of the information provided as stated below.

[4] https://www.regierung.li/files/medienarchiv/784-13-30-06-2023-en.pdf

According to Art. 13 (1) lit. f, i, k and l CSG the submitted notifications can be used to exchange information (in a responsible manner) with national and international authorities, so that they can perform tasks within their sphere of influence, take measures and mitigate or even eliminate threats. According to Art. 13 (1) lit. d CSG information may be disclosed to safeguard the security of network and information systems or to prevent security incidents.

According to Art. 13 (1) lit. h CSG in relation to Art. 5 (5) CSG the CSIRT.LI as department of the SCS may notify the public about concrete security incidents if raising awareness seems necessary for the prevention of security incidents or for the management of current security incidents, after consultation of the affected constituent.

In incident handling the main purpose of CSIRT.LI is the coordination of incident response. After receiving a notification of a risk or security incident CSIRT.LI may give non-binding recommendations to the constituency.

As a national CSIRT we do not have any police authority, which is why we cannot legally enforce actions to be taken by an Internet Service Provider (ISP), like takedowns for example. If we think it could be promising, we will contact the provider or a national/international partner and raise our concerns.

4. Policies

4.1 Types of incidents and level of support

CSIRT.LI may act upon request of one of its constituents or may act if one of its constituents is involved in an information security incident. Note that support must in general be actively requested by the affected constituent. Only limited support can be given to end users.

The level of support given by CSIRT.LI will vary depending on the type and severity of the incident, vulnerability or issue as determined by CSIRT.LI staff, the type of asset or constituent affected and CSIRT.LI's resources at the time, especially through:

- Advice and assistance, particularly by providing general guidance on mitigation and recovery strategies. Note that CSIRT.LI is not a helpdesk.
- Coordination activities and referral to national and international maintained contacts who can potentially assist with recommendations or technical support, as well as through information sharing.

CSIRT.LI will do its best to keep its constituency informed about potential severe vulnerabilities and where possible will inform (especially via mailing list) before they are actively exploited.

Overall, the primary role of CSIRT.LI in case of an incident is the exchange of information and coordination and not on-site incident response. It is to be mentioned that neither the SCS nor the CSIRT.LI shall compete with private sector providers. The effective on-site incident handling is up to local security teams and commercial providers.

4.2 Co-operation, Interaction and Disclosure of Information

The core task of the national CSIRT.LI includes reporting incidents to national CSIRTs in other countries to deal with all sites involved in handling large-scale cyber-attacks. Beyond that, CSIRT.LI is interested in responsible information exchange with various other national and foreign stakeholders as well as communities concerning the global field of cyber security, which could impact Liechtenstein.

CSIRT.LI will protect the privacy of reporters, partners and our constituents by usually passing on information in an anonymised way, except the fulfilment of a specific task cannot be ensured or other contractual agreements or laws apply.

As described in 3.4 CSIRT.LI is authorized by law to notify the public about concrete security incidents if raising awareness is necessary for the prevention of security incidents or for the management of current security incidents, after consultation of the affected constituent. Depending on the case, the identity of the constituent will be anonymised, if this does not undermine the purpose of the notification.

CSIRT.LI operates under the restrictions imposed by Liechtenstein law. This involves careful handling of personal data as required by Liechtenstein Data Protection law.

CSIRT.LI uses the Traffic Light Protocol (TLP)[5] in Version 2.0 when sharing information with teams that support it and will honour such information if present.

CSIRT.LI is a member of FIRST, the Forum of Incident Response and Security Teams and is listed on Trusted Introducer (TI).

4.3 Communication and authentication

For communication of unclassified or low-sensitive data, CSIRT.LI prefers to use unencrypted e-mail for reasons of traceability. For secure communication with CSIRT.LI make use of the information provided on the contact page. A contact form for secure submission of general requests (with file transfer possibility) and a form for notifications about security incidents are currently available. It is also possible to make use of PGP and S/MIME encrypted e-mail and telephone.

If there is a desire to use PGP or S/MIME encrypted e-mail communication, it would be useful to exchange keys (especially in the case of PGP) before an incident occurs, to avoid time delays in case of emergency.

If it's necessary to authenticate a person before communicating, this can be done either through existing networks of trust (e.g. FIRST, TI) or by other methods like call-back, mail-back or even face-to-face meeting if necessary.

CSIRT.LI can be reached by telephone during operating hours.

[5] https://www.first.org/tlp/

5. Services

CSIRT.LI supports the members of its constituency with a set of reactive and proactive services.

In networking, cooperation and coordination, particularly with other national CSIRTs, as well as private individuals and players from business, the main task is information gathering and its distribution. This is to be done by responding to cyber-security-related requests, creating situation reports, warnings and alerts. Technical analyses or the analysis of individual cases is not foreseen. The CSIRT.LI as a government agency is not supposed to compete with private-sector providers and does not take an active role in technical remediation or mitigation.

5.1 Incident response

As stated in Art. 19 CSG incident response is carried out in the form of incident triage, incident coordination and incident resolution.

5.1.1 Incident triage

- Conducting investigations to confirm the occurrence of an incident, primarily by assisting in the analysis and interpretation of information collected and provided by the affected constituent.
- Assessing and prioritizing the incident.

5.1.2 Incident coordination

- Connecting the constituent to specialists who can potentially assist with recommendations or technical support.
- If useful sharing information with other CSIRTs or contacting other parties which can help to mitigate or resolve the incident.
- Asking for reports.
- Reporting back.

5.1.3 Incident resolution

- Providing advice and guidance on mitigation and recovery strategies if required, mainly through providing supportive documents on the CSIRT.LI's website or through referencing on partner-websites.
- Maintain communication with local security teams (such as internal CSIRTs) and engage with constituents as long as it aligns with the CSIRT's responsibilities and can be accommodated by the available staff.

5.2 Proactive activities

To the extent that this is feasible, especially in terms of human resources, partly dependent on cooperation with private and governmental partner organizations and their willingness to share information.

- Continuously monitoring of public and restricted accessible information about vulnerabilities in order to issue alerts to the constituency.
- If information about a specific risk is coming to the attention of CSIRT.LI, it will be passed on to the affected constituent.

- Provide possibilities for community building and information exchange within the constituency to support self-empowerment and increase risk awareness.
- Provide information on current events, attack and defense trends, or emerging technologies that may impact constituent security posture.

5.3 Incident notification form

A web form to notify about security incidents ("notification form") is provided under the following link:
https://www.llv.li/en/national-administration/national-cyber-security-unit/incident-notification (en)
https://www.llv.li/de/landesverwaltung/stabsstelle-cybersicherheit/it-sicherheitsvorfall-melden (de)

5.4 Service levels

CSIRT.LI aims to react to incoming incident notifications from humans within one business day.

6. Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, CSIRT.LI assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.

FÜRSTENTUM LIECHTENSTEIN LANDESVERWALTUNG	**This document was signed with an official signature.**
	National Cyber Security Unit Peter Wohlgenannt
	2024-03-21 12:46:48 +01:00
	Information about the verification of the electronic signature can be found at: www.llv.li/signaturpruefung
	According to Art. 24a Abs. 3 E-Government-Act a printout of this document has the presumption of being genuine.