RFC 2350: CERT.LV Description

Version 5.4

Document OID: 1.3.6.1.4.1.28446.2.1.5.4

1. About this document

1.1 Date of Last Update

This is version 5.4 published on 27/06/2019

1.2 Distribution List for Notifications

Currently, CERT.LV has not established a mailing list to notify updates of this document. Major updates are communicated via CERT.LV website news section and social networks Twitter and Facebook.

1.3 Locations where this Document May Be Found

The current version of this CERT.LV description document is available from the CERT.LV WWW site: **https://www.cert.lv/lv/par-mums** and **https://www.cert.lv/en/about-us**

1.4 Identification

1. Document title: "CERT.LV Description"

2. Version: 5.4.

3. Document Date: 27.06.2019.

4. OID: 1.3.6.1.4.1.28446.2.1.5.4

IANA	1.3.6.1.4.1
IMCS UL	28446
CERT.LV	.2
Description	.1
Major Version	.5
Minor Version	.4

5. Expiration: This document is valid until further notice.

2. Contact Information

2.1 Name of the Team

CERT.LV: Information Technologies Security Incident Response Institution of the Republic of Latvia.

CERT.LV formerly known as CERT NIC.LV and LATNET CERT was established on 01 August 2006.

DDIRV (National Computer Security Incident Response Team) was merged with CERT NIC.LV on 1 February 2011 to form CERT.LV.

2.2 Address

CERT.LV
Raiņa bulvāris 29
Rīga, LV-1459
Latvia

2.3 Time Zone

Eastern European Time [EET]: GMT+0200

Daylight Savings Time: GMT+0300 (from last Sunday in March till last Sunday in October).

2.4 Telephone Number

+371 67085888

2.5 Facsimile Number

+371 67225072 (this is **not** a secure fax)

2.6 Other Telecommunication

None available

2.7 Electronic Mail Address

cert@cert.lv is the main address for incident reporting.

All emails are processed using the incident tracking system and ticket numbers will be assigned. It is recommended to use the assigned ticket numbers for all communication concerning the same incident. New incidents shall never re-use an already assigned ticket number.

2.8 Public Keys and Other Encryption Information

The CERT.LV has a PGP key, the details:

User ID: CERT.LV

Key ID: 0x87BCCEEDC0DE2EC3

Key type: RSA

Key size: 4096 bit

Expiration: Never

Fingerprint: B5E8 82A1 338E 7749 09D0 A8F0 87BC CEED C0DE 2EC3

The key and its signatures can be found here: **https://www.cert.lv/en/contacts** and at the usual large public key servers.

2.9 Team Members

Baiba Kaškina is the Head of CERT.LV.

Varis Teivāns is the Deputy Head of CERT.LV.

Information about other team members is available online on the CERT.LV webpage.

2.10 Other Information

General information about the CERT.LV, as well as details on CERT.LV activity areas and links to various recommended security resources, can be found at **https://www.cert.lv**

Most information is available in Latvian only.

2.11 Points of Customer Contact

The preferred method for contacting CERT.LV is via email to **cert@cert.lv**. We encourage our constituents to use PGP encryption when sending any sensitive information to CERT.LV.

Our regular response hours are workdays 09:00 – 18.00 (local time, save public holidays in Latvia). Reporting of incidents is possible by telephone 24x7. The person on duty will involve CERT.LV specialists as needed.

3. Charter

3.1 Mission Statement

The mission of CERT.LV is to improve and promote the overall information technologies security in Latvia by focussing on the following objectives:

- maintain common electronic information space monitoring;
- provide support in information technologies security incident response and coordinate their prevention;
- maintain in a publicly accessible way in line with the actual threats recommendations on the current information technologies risks;
- conduct research, organize educational events, education and training in the field of information technologies security;
- provide support to state institutions in safeguarding national security, as well as crime and other crime detection (investigation) in the field of information technologies, complying with statutory restrictions on data processing;
- monitor state and local government institutions and telecommunication operators compliance with the duties in the field of information technologies security;
- cooperate with internationally recognized information technology security incident prevention institutions (teams, CSIRTs/PSIRTs);
- handle incident reporting in the context of the NIS directive (Network and Information Security directive) and cooperate with Operators of Essential Services, Digital Service Providers, Single point of contact and the Competent Authority in Latvia as well as NIS CSIRT Network internationally;
- carry out other obligations under laws and regulations.

3.2 Constituency

CERT.LV primary constituency are:

- state institutions and local authorities of Latvia;
- Operators of Essential Services and Digital Service Providers on the context of NIS directive;
- IT Critical infrastructure of Latvia.

CERT.LV secondary constituency are:

- private sector using IP addresses of Latvia and resources with TLD .lv;
- citizens using IP addresses of Latvia and resources with TLD .lv.

The list of IP addresses of Latvia can be found at: **http://www.nic.lv/lix**

3.3 Sponsorship and/or Affiliation

The CERT.LV is financed and supervised by the Ministry of Defence of the Republic of Latvia.

CERT.LV is mandated by the IT Security Law to represent Latvia in the NIS CSIRTs Network.

CERT.LV is actively taking part in the GEANT's Task Force TF-CSIRT.

CERT.LV is certified by the Trusted Introducer since September 2016 (and accredited since May 2008).

CERT.LV is full member of FIRST since April 2009.

3.4 Authority

CERT.LV operates under the auspices of Institute of Mathematics and Computer Science, University of Latvia, with authority delegated by and under supervision of the Ministry of Defence of the Republic of Latvia.

Information technologies security law empowers CERT.LV:

- to request disconnection of an end user if the user threatens rights of other users or their information systems or security of electronic communication networks;
- to request from the highest level ".lv" domain name registrar and electronic numbering system maintainer of ".lv" to disconnect a domain name in case this domain name is involved in a cybersecurity incident, that significantly threatens the security of information system or electronic communications networks and in the case the cybersecurity incident cannot be resolved in any other way. Once requesting the disconnection CERT.LV indicates the duration of the disconnection. This does not exceed 5 days. In case any additional actions need to be taken by the registrar and the numbering system maintainer, then these are requested accordingly;
- to request the Ministry of Defence of the Republic of Latvia to inform single point of contact from another EU Member State about cybersecurity incidents, that significantly threatens the security of information system or electronic communications networks and concerns the operators of essential services and/or digital service providers;
- CERT.LV can take compulsory decisions, to ensure public institutions and private entities are compliant with duties imposed by the law.

4. Policies

4.1 Types of Incidents and Level of Support

The CERT.LV is authorized to address all types of IT security incidents which occur, or threaten to occur, at all networks in Latvia. An IT Security incident (hereinafter - Incident) is a harmful event or offense that endangers the integrity, availability or confidentiality of information technology. Issues and events related to content i.e. copyright are not considered incident from CERT.LV point of view.

Incidents are prioritized according to type and the severity of the incident. Incidents directly affecting primary constituency are treated with higher priority.

The level of support given by CERT.LV will vary depending on the type of constituent, type and severity of the incident or issue, the size of the user community affected, and CERT.LV resources at the time; though in all cases some meaningful response will be made within one working day.

CERT.LV will provide support also for the end users, however it is preferred if they contact their system administrator, network administrator, or department head for assistance before contacting CERT.LV.

CERT.LV services are provided on a best effort basis.

In case of crisis within the primary constituency (see point 3.2.), the response times will be longer for incidents coming from the secondary constituency.

CERT.LV uses international version of incident classification/incident taxonomy which is published:

https://www.trusted-introducer.org/processes/standards.html

4.2 Co-operation, Interaction and Disclosure of Information

CERT.LV maintains and moderates cooperation with Latvian ISPs CSIRT and abuse teams as well as with law enforcement representatives. CERT.LV is one of the founders of the DEG initiative (Information Technology and Information Systems Security Experts Group).

CERT.LV will share information on a need-to-know basis, and where required by regulations in an anonymized fashion when this will assist appropriate entities in resolving or preventing security incidents.

Information being considered for release will be classified as follows:

- Private user information will not be released in identifiable form outside the CERT.LV, except as provided below. If the identity of the user is disguised, then the information can be released freely.

- Intruder information, and in particular identifying information will not be released to the public (unless it becomes a matter of public record, for example because criminal charges have been laid), it will be anonymized and will be exchanged freely with system administrators and CSIRTs tracking the incident.
- Private site information will not be released without the permission of the site in question, except as provided below.
- Vulnerability information will be released freely, though according to internal procedure every effort will be made to inform the relevant vendor before the general public is informed.
- Statistical information will be released at the discretion of the CERT.LV. CERT.LV publishes monthly and quarterly statistics on the website.
- Contact information on the institutions and organizations will be released freely, except where the contact person or entity has requested that this not be the case, or where CERT.LV has reason to believe that the dissemination of this information would not be appreciated. Contact information of private users will not be shared with third parties.

Potential recipients of information from the CERT.LV will be classified as follows:

- Constituency: entitled to receive whatever information is necessary to facilitate the handling of computer security incidents which occur in their jurisdictions.
- System administrators / responsible persons for the IT security within the constituency, by virtue of their responsibilities, trusted with confidential information.
- Users within the constituency are entitled to information which pertains to the security of their own computer accounts. Users within the constituency are entitled to be notified if their account is believed to have been compromised.
- The CERT.LV constituencies will not receive restricted information, except where the affected parties (legitimate owners, operators, and users of the relevant computing facilities) have given permission for the information to be disseminated.
- The IT security community will be treated the same way the general public is treated. Exceptions can be made regarding Trusted Introducer community of accredited and certified CSIRTs, NIS CSIRT Network as well as FIRST members. While members of CERT.LV may participate in discussions within the computer security community, such as newsgroups, mailing lists and conferences, they will treat such forums as though they were the public at large. While technical issues (including vulnerabilities) may be discussed to any level of detail, any examples taken from

CERT.LV experience will be disguised to avoid identifying the affected parties. In case more sensitive information is discussed in closed meetings or discussion lists, TLP protocol will be used to mark information dissemination expectations.

- The press will also be considered as part of the general public. CERT.LV will provide comments and give interviews regarding vulnerabilities, computer security incidents, and general computer security topics without disclosing sensitive information that might help to identify involved organizations or individuals.
- Other sites and CSIRTs, when they are partners in the investigation of a computer security incident, will in some cases be trusted with confidential information. This will happen only if the foreign sites bona fide can be verified, and the information transmitted will be limited to that which is likely to be helpful in resolving the incident. For the purposes of resolving a security incident, otherwise semi-private but relatively harmless user information such as the provenance of connections to user accounts will not be considered highly sensitive, and can be transmitted to a foreign site without excessive precautions.
- Law enforcement officers will receive full cooperation from the CERT.LV, according to legislation requirements including any information they require to pursue an investigation, notwithstanding the earlier statements made about confidentiality.

CERT.LV understands and supports the traffic light protocol (TLP **https://www.first.org/tlp**).

4.3 Communication and Authentication

In view of the types of information that the CERT.LV will likely be dealing with, telephones will be considered sufficiently secure to be used even unencrypted. Unencrypted e-mail will not be considered particularly secure, but will be sufficient for the transmission of low-sensitive data. If it is necessary to send highly sensitive data by e-mail, PGP will be used. Network file transfers will be considered to be similar to e-mail for these purposes: sensitive data should be encrypted for transmission.

Where it is necessary to establish trust, for example before relying on information given to the CERT.LV, or before disclosing confidential information, the identity and bona fide of the other party will be ascertained to a reasonable degree of trust. Within constituency, and with known neighbour sites, referrals from known trusted people will suffice to identify someone. Otherwise, appropriate methods will be used, such as a search of FIRST members or Trusted Introducer data base, the use of WHOIS and other Internet registration information, etc. along with telephone call-back or e-mail mail-back to ensure that the party is not an impostor. Incoming e-mail whose data must be trusted will be checked with the originator personally, or by means of digital signatures (PGP in particular) is supported.

4.4 Information handling

Information is stored according to the following procedure:

- in paper form – it is stored in dedicated folders/safe (depending on classification) in the CERT.LV working room which is protected with electronic door card;
- in electronic form – it is stored on CERT.LV servers and workstations, protected with all normal security measures.

Information is archived according to the following procedure:

- in paper form – it is archived in dedicated folders/safe (depending on classification) in the CERT.LV working room which is protected with electronic door card;
- in electronic form – it is archived on CERT.LV servers, protected with all normal security measures.

Information is destructed according to the following procedure:

- in paper form – it is destructed in the shredder;
- in electronic form – it is destructed by deleting and overwriting using special software.

5. Services

Services offered by CERT.LV can be grouped into the following categories:

- reactive services, i.e., services that are initiated by an incident;
- proactive services, i.e., services aimed to provide necessary help in protecting and securing networks and computer systems against possible attacks;
- awareness raising and educational services, i.e., training seminars, provision of information and distribution of educational materials in order to raise awareness about computer security issues in order to reduce the number of incidents.

All above mentioned services are provided free of charge.

5.1 Incident Response

CERT.LV offers the following reactive services:

- 24x7 assistance in incident handling and response;
- Co-ordination of incident handling with other CSIRT and security teams in Latvia and abroad, as well as with local authorities.

CERT.LV will assist system administrators in handling the technical and organizational aspects of incidents response. In particular, it will provide assistance or advice with respect to the following aspects of incident management:

5.1.1 Incident Triage

- investigating whether indeed an incident occurred;
- determining the extent of the incident.

5.1.2 Incident Coordination

- determining the initial cause of the incident (vulnerability exploited);
- facilitating contact with other sites which may be involved;
- facilitating contact with appropriate law enforcement officials, if necessary;
- making reports to other CSIRTs, if applicable;
- composing announcements to users, if applicable.

5.1.3 Incident Resolution

Providing assistance to:

- removing the vulnerability;
- securing the system from the effects of the incident;
- in specific cases, forensic analysis of the affected site.

In addition, CERT.LV will collect statistics concerning incidents which occur within or involve its constituency, and will notify the community as necessary to assist it in protecting against known attacks.

To make use of CERT.LV incident response services, please send e-mail as per section 2.11 above.

Please remember that the amount of assistance available will vary according to the parameters described in section 4.1.

5.2 Proactive Activities

CERT.LV offers the following proactive services:

- assistance in implementation of proactive defence against attacks;
- consultations regarding configuration and maintenance of security monitoring tools and applications as well as requirements for public procurement;
- pentesting (if applicable);
- provisioning of early detection system instance (if applicable);
- DNS Firewall service (if applicable);
- MISP information sharing service (if applicable);
- detection of intrusion incidents.

5.3 Awareness raising services

CERT.LV offers the following awareness raising services:

- lectures on IT security related topics in state and governmental institutions;
- lectures on IT security topics in schools and universities;
- participation in various events that are promoting IT security, e.g., Safer Internet Day, E-skills Week, European Cyber Security Month;
- participation in public discussions on IT security related subjects;
- organisation of the annual security conference "Kiberšahs";
- organisation of bi-annual seminars for IT security professionals "Be safe";
- organisation of security specialists meetings and discussions;
- organisation of seminars on various security related issues;
- maintenance of websites **www.cert.lv** (official website) and **www.esidross.lv** (for general public);
- active information sharing in social media (on Facebook, Twitter);
- dissemination of security related materials in mass media;
- joining organizations that promote cybersecurity;
- preparing brochures and posters for schools and public use on IT security related topics;
- recommendations for vulnerability avoidance.

The CERT.LV coordinates and maintains the following information services to the extent possible depending on its resources:

- information services;
- NTP Stratum - 1 level time clock service;
- Incident statistics. Records of security incidents handled will be kept. While the records will remain confidential, periodic statistical reports will be made available to on-line.

6. Incident Reporting Forms

There are no special forms required to report an incident. The preferred way of reporting is by email.

7. Disclaimers

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