

# CERT.LV Description

*Version 3.1*

*Document OID: 1.3.6.1.4.1.28446.2.1.3.1*

## 1. About this document

### 1.1 Date of Last Update

This is version 3.1 published on 3 May 2011.

### 1.2 Distribution List for Notifications

Currently, CERT.LV has not established mailing list to notify updates of this document.

### 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; its URL is:

[http://www.cert.lv/uploads/uploads/CERT\\_LV-description\\_v-3.1.pdf](http://www.cert.lv/uploads/uploads/CERT_LV-description_v-3.1.pdf)

### 1.4 Authenticating this Document

This document has been signed with the CERT.LV's PGP key. The signature is also available on our Web site, under:

[http://www.cert.lv/uploads/uploads/PGP/CERT\\_LV-description\\_v-3.1.pdf.sig](http://www.cert.lv/uploads/uploads/PGP/CERT_LV-description_v-3.1.pdf.sig)

### 1.5 Identification

1. Document title: "CERT.LV Description"

2. Version: 3.1.

3. Document Date: 03.05.2011

4. OID: 1.3.6.1.4.1.28446.2.1.3.1

IANA 1.3.6.1.4.1

IMCS UL 28446

CERT.LV .2

Description .1

Major Version .3

Minor Version .1

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 joined to CERT NIC.LV on 1 February 2011 to establish CERT.LV.

## 2.2 Address

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

## 2.3 Time Zone

Eastern European Time GMT+0200 DST: GMT+0300 (from last Sunday in March till last Sunday in October)

## 2.4 Telephone Number

+371 67085858

## 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](mailto:cert@cert.lv), [cert@cert.gov.lv](mailto:cert@cert.gov.lv), [abuse@cert.lv](mailto:abuse@cert.lv), [abuse@cert.gov.lv](mailto:abuse@cert.gov.lv)

These emails are distributed to the CERT.LV team and also filed in the incident tracking system with 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: 0xE49D332C Key type: DH/DSS  
Key size: 4096/1024 bit Expiration: Never

Fingerprint: EBBE 32C8 243B B714 E1FB 2EDF DBDA ACC3 E49D 332C

The key and its signatures can be found at the usual large public key servers.

## **2.9 Team Members**

Baiba Kaškina is the head of CERT.LV.

Other members of the team are:

Artūrs Medenis

Varis Teivāns

Kristians Meliņš

Gints Mālkalnetis

Māris Kalējs

Egīls Stūrmanis

Ģirts Mažonis

Iveta Skujiņa

Ivo Ķutts

## **2.10 Other Information**

General information about the CERT.LV, as well as links to various recommended security resources, can be found at <http://www.cert.lv>

## **2.11 Points of Customer Contact**

The preferred method for contacting the CERT.LV is via email to [cert@cert.lv](mailto:cert@cert.lv). The received information will be handled by the responsible human. We encourage our constituents to use PGP encryption when sending any sensitive information to CERT.LV.

If it is not possible (or not advisable for security reasons) to use e-mail, the CERT.LV can be reached by telephone during regular office hours. In case of an emergency it is possible to reach person on duty who will involve CSIRT specialists as needed.

If possible, when submitting your report, use the form mentioned in section 6.

# **3. Charter**

## **3.1 Mission Statement**

Mission of the CERT.LV is to improve and promote the overall information technologies security in Latvia.

### **3.1.1. Main Objectives**

Objectives of CERT.LV are to:

- maintain common electronic information space monitoring;

- provide support in information technologies security incident prevention or 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 technologies security incident prevention institutions (teams) (CSIRTS);
- carry out other obligations under laws and regulations.

### **3.2 Constituency**

CERT.LV's constituency is IP addresses of Latvia and all resources with TLD .lv. The list of addresses can be found at: <http://www.nic.lv/lix>.

### **3.3 Sponsorship and/or Affiliation**

The CERT.LV is financed by the Ministry of Transport of the Republic of Latvia.

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

CERT.LV is the TI accredited team since May 2008.

CERT.LV is the 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 Transport 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. It also empowers CERT.LV to take compulsory decisions, to ensure public institutions and private entities compliance 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 computer security incidents which occur, or threaten to occur, at all networks in Latvia.

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

Resources will be assigned according to the following priorities, listed in decreasing order:

- Attacks on critical infrastructure
- Attacks on Internet infrastructure, e.g. root or system-level attacks on any Server System, or any part of the backbone network infrastructure, denial of service attacks
- Deliberate persistent attacks on specific resources, i.e. any compromise which leads or may lead to unauthorized access of systems
- Widespread automated attacks against Internet sites, e.g. sniffing attacks, IRC "social engineering" attacks, password cracking attacks
- Threats, harassment, and other criminal offences involving individual user accounts
- New types of attacks or new vulnerabilities
- Botnets, i.e. activities related to network of compromised systems controlled by attacker
- Denial of service on individual user accounts, e.g. mail bombing
- Forgery and misrepresentation, and other security-related violations of local rules and regulations, e.g. e-mail forgery, SPAM and etc.
- Compromise of single desktop systems

Types of incidents other than those mentioned above will be prioritized according to their apparent severity and extent.

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 the CERT.LV.

CERT.LV services are provided as the best effort.

### **4.2 Co-operation, Interaction and Disclosure of Information**

CERT.LV maintains and moderates cooperation with Latvian ISP's CSIRT and abuse teams as well as with law enforcement representatives. CERT.LV is behind the LV-CSIRT initiative (more info: <http://www.csirt.lv/>).

While there are legal and ethical restrictions on the flow of information from CERT.LV, the CERT.LV acknowledges its indebtedness to, and declares its intention to contribute to, the spirit of cooperation that created the Internet. Therefore, while appropriate measures will be taken to protect the identity of members of our constituency and members of neighbouring sites where necessary, the CERT.LV will otherwise share information freely when this will assist others in resolving or preventing security incidents.

In the paragraphs below, "affected parties" refers to the legitimate owners, operators, and users of the relevant computing facilities. It does not refer to unauthorized users, including otherwise authorized users making unauthorized use of a facility; such intruders may have no expectation of confidentiality from the CERT.LV. They may or may not have legal rights to confidentiality; such rights will be respected where they exist.

Information being considered for release will be classified as follows:

- Private user information will be not released in identifiable form outside the CERT.LV, except as provided for 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 an incident.
- Private site information will not be released without the permission of the site in question, except as provided for below.
- Vulnerability information will be released freely, though 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.
- Contact information 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.

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

- Constituencies: entitled to receive whatever information is necessary to facilitate the handling of computer security incidents which occur in their jurisdictions.
- System administrators 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 have given permission for the information to be disseminated. Statistical information may be made available to the general CERT.LV constituencies. There is no obligation on the part of the CERT.LV to report incidents to the constituencies, though it may choose to do so.
- The computer security community will be treated the same way the general public is treated. 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.

- The press will also be considered as part of the general public. The CERT.LV will not interact directly with the Press concerning computer security incidents, except to point them toward information already released to the general public. The above does not affect the ability of members of CERT.LV to grant interviews on general computer security topics; in fact, they are encouraged to do so, as a public service to the community.
- 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. "Intruder information" will be transmitted freely to other system administrators and CSIRTs.
- Law enforcement officers will receive full cooperation from the CERT.LV, including any information they require to pursue an investigation, notwithstanding the earlier statements made about confidentiality.

The constituencies of CERT.LV are entitled to receive all kind of information, which is needed for solving security incidents, except the private user information. In case of private site information, the information will be released only if the permission would be given.

### **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-sensitivity 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, 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 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 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 services, i.e., 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;
- co-ordination of incident handling with other CSIRT teams in Latvia and abroad, as well as with local authorities;
- vulnerability analysis;
- artefact analysis.

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's 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;
- configuration and maintenance of security monitoring tools and applications;
- detection of intrusion incidents.

## **5.3 Awareness raising services**

CERT.LV offers the following awareness raising services:

- organisation of security specialists meetings and discussions;
- maintenance of security alert e-mail list;

- organisation of seminars on various security related issues;
- dissemination of security related materials in mass media.

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

- Information services
- List of all Latvian ISP' abuse teams contact addresses
- Records of security incidents handled will be kept. While the records will remain confidential, periodic statistical reports will be made available to the CERT.LV constituency and on-line.

## **6. 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.