LITNET CERT
https://cert.litnet.lt

CSIRT Description for LITNET CERT

1. About this document

This document describes the computer security response functions of the Computer Emergency Response Team (CERT) of Lithuanian Academic and Research Network (hereafter referred to as LITNET) in accordance with RFC 2350.

1.1 Date of Last Update

This is version 1.5, published on August 2 2017.

1.2 Distribution List for Notifications

LITNET CERT does not use any distribution list to notify about changes this document.

1.3 Locations where this Document May Be Found

The current version of the CERT description document is available at https://cert.litnet.lt/about/

Please make sure you are using the latest version.

1.4 Authenticating this document

This document has been signed with the LITNET CERT's PGP key. The signatures also can be found at https://cert.litnet.lt/about/ .

2. Contact Information

2.1 Name of the Team

„LITNET CERT" : The Computer Emergency Response Team of LITNET

2.2 Address

LITNET CERT
Studentu 48a-101
51367, Kaunas
Lithuania

2.3 Time Zone

Eastern Europe Time (GMT+0200 and GMT+0300 from last Sunday in March till last Sunday in October)

2.4 Telephone Number

+370 37 300 645

2.5 Facsimile Number

+370 37 300 643

2.6 Other Telecommunication

None available.

2.7 Electronic Mail Address

<cert@litnet.lt> This is a e-mail alias that relays mail to the LITNET CERT team members.

2.8 Public Keys and Other Encryption Information

The LITNET CERT has a PGP key, with KeyID: 0x8A314930 and fingerprint: ECD2 DE50 DD2F 01BD F164 51CB AE51 0C14 8A31 4930

The key and its signatures can be found at public key servers like pgp.mit.edu.

2.9 Team Members

LITNET CERT consists of six working groups, which are located in LITNET Technical centres. Each working group has at least one person – LITNET CERT member. LITNET CERT working groups and members are listed on the LITNET website https://cert.litnet.lt/lt/kontaktai

Milda Mimiene (LITNET KTU Technical Centre) is the LITNET CERT coordinator.

2.10 Other Information

General information about the LITNET CERT, as well as links to various recommended security resources, can be found at https://cert.litnet.lt

2.11 Points of Customer Contact

The preferred method for contacting the LITNET CERT is via e-mail cert@litnet.lt. The responsible LITNET CERT team member will handle e-mails sent to this address.

If it is not possible (or not advisable or not allowed for security reasons) to use e-mail, the LITNET CERT can be reached by telephone during regular office hours.

The LITNET CERT's hours of operation are generally restricted to regular business hours (09:00-17:00 Monday to Friday except public holidays).

3. Charter

3.1 Mission Statement

The purpose of the LITNET CERT is to provide the capability to computer security incidents in LITNET network.

3.2 Constituency

The LITNET CERT's constituency is all institutions connected to LITNET network (AS2847 and AS5479).

3.3 Sponsorship and/or Affiliation

LITNET CERT operates as a part of Lithuanian Research and Education Computer Network (LITNET) services funded by Ministry of Education of Respublic of Lithuania.

LITNET CERT is full member of FIRST (Forum of Incident Response and Security Teams) since 2003.
LITNET CERT is accredited by the Trusted Introducer since January 2005 and taking part in the GEANT's Task Force TF-CSIRT.

3.4 Authority

LITNET CERT operates under the auspices of, and with authority delegated by, the Board of Lithuanian Research and Education Computer Network (LITNET).

LITNET CERT aims to work cooperatively with the IT system administrators and users of institutions connected to LITNET, and, as much as possible, to avoid authoritarian relationships. However, should circumstances warrant it, the LITNET CERT has the authority to take the measures it deems appropriate to properly handle a computer security related incident.

4. Policies

4.1 Types of Incidents and Level of Support

LITNET CERT is authorized to address all types of computer security incidents that occur, or threaten to occur, in LITNET network.

The level of support given by LITNET CERT 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 LITNET CERT's resources at the time, though in all cases some response will be made within one working day. Communication methods are in place to inform the owners of infrastructure up to the government level. As a general rule, no end-user support is offered.

The LITNET CERT is committed to keeping the LITNET system administration community informed of potential vulnerabilities, and where possible, will inform the community of such vulnerabilities before they are actively exploited.

LITNET CERT will keep a record of a list of persons from each institution that is known to LITNET CERT to be in charge of the security policies and operations.

4.2 Co-operation, Interaction and Disclosure of Information

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

LITNET CERT highly regards the importance of operational cooperation and information-sharing between the CERT‘s and other organisations that may contribute to or make use of their services.

LITNET CERT operates within the confines imposed by the legislation of Respublic of Lithuania.

LITNET CERT supports the Information Sharing Traffic Light Protocol (ISTLP – see https://www.trusted-introducer.org/ISTLPv11.pdf): - information that comes with the tags WHITE, GREEN, AMBER or RED will be handled appropriately.

4.3 Communication and Authentication

In view of the types of information that the LITNET CERT will likely be dealing with, telephones will be considered sufficiently secure to be used even unencrypted. Unencrypted e-mails 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 and not provide sufficient security for data transfer. For secure transmission sensitive data should be encrypted.

The identity and bona fide of the other party will be ascertained to a reasonable degree of trust, where it is necessary to establish the trust, for example before relying on information given to the LITNET CERT, or before disclosing confidential information. 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 Introduser data base, the use of WHOIS and other Internet registration information, etc. to ensure that the party is not an impostor. The content of 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).

5. Services

5.1 Incident Response

LITNET CERT will assist system administrators in handling the technical and organizational aspects of incidents. 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 that may be involved.
- Facilitating contact with the affected constituent and/or appropriate law enforcement officials, if necessary.
- Making reports to other CSIRTs, if applicable.
- Composing announcements to users, if applicable.

5.1.3 Incident Resolution

- Recommendations on removing vulnerability.
- Securing the system from the consequences of the incident.
- Collecting the evidence of the incident.

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

To make use of LITNET CERT’s incident response services, please send an 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

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

- Information services
    - Mailing lists to inform security contacts of new information relevant to their computing environments. These lists will be made available only to the system administrators within the constituency.

- Auditing services
    - Security level of machines within constituency networks will be assessed on demand.
- Archiving services
    - Records of security incidents handled will be kept. While the records will remain confidential, periodic statistical reports will be made available to the public.

6. Incident Reporting Forms

LITNET CERT online incident reporting form is available at https://cert.litnet.lt/report-an-incident/ .

7. Disclaimers

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