CYBERCIRCLE

CYBER CIRCLE CSIRT

RFC 2350

Document Control

From: CYBER CIRCLE CSIRT
Version: 2.0
Date: 2023-03-23

Document location https://cybercircle.eu/about

Document Classification PUBLIC / TLP:CLEAR

Contents

1. Document Information

This document contains a description of CYBER CIRCLE CSIRT as implemented by RFC 2350. It provides basic information about CYBER CIRCLE CSIRT, its channels of communication, its roles and responsibilities.

1.1. Date of Last Update

Version 2.0, published on 23rd March 2023.

1.2. Distribution List for Notifications

There is no distribution list for notifications.

1.3. Locations where this Document May Be Found

The current and latest version of this document is available at:

https://cybercircle.eu/about

1.4. Document Authenticity

This document has been signed with the PGP key of CYBER CIRCLE CSIRT. The signature is available on CYBER CIRCLE CSIRT's website. Its URL is:

https://cybercircle.eu/about

1.5. Document Identification

Title: "CYBER CIRCLE CSIRT RFC 2350".

Version: 2.0.

Document date: 2023-03-23.

Expiration: this document is valid until superseded by a later version.

2. Contact Information

2.1. Name of the Team

CYBER CIRCLE CSIRT

2.2. Address

CYBER CIRCLE CSIRT

Rīgas iela 20 – 22, Valmieras nov., Valmiera, LV-1042, Latvia.

2.3. Time Zone

EET, Eastern European Time (UTC+2, between last Sunday in October and last Sunday in March).

EEST, Eastern European Summer Time (UTC+3, between last Sunday in March and last Sunday in October).

2.4. Telephone Number

+371 26338522

2.5. Facsimile Number

Not applicable.

2.6. Other Telecommunication

Not applicable.

2.7. Electronic Mail Address

Please use below email to send incident reports and/or cyber threat operational matters:

- csirt@cybercircle.eu

This is a e-mail alias that relays mail to the human(s) on duty for the CYBER CIRCLE CSIRT.

2.8. Public Keys and Encryption Information

Key ID: 0x5c6569c3625b1dd6

Fingerprint: 6331 4E01 7256 6D37 DAD4 836D 5C65 69C3 625B 1DD6

Key type: RSA/2048

Expires: 2027-02-06

The key is available on the usual public key servers such as https://pgp.circl.lu/

2.9. Team Members

The head of CYBER CIRCLE CSIRT is Aleksandrs Orlovs.

CYBER CIRCLE CSIRT team is composed of IT security experts. The list of CYBER CIRCLE CSIRT team's members is not publicly available. The identity of CYBER CIRCLE CSIRT team's members might be divulged on a case-by-case basis according to the need-to-know restrictions.

2.10. Team Members

General information about CYBER CIRCLE is available at https://cybercircle.eu/

2.11. Points of Customer Contact

The preferred method to contact CYBER CIRCLE CSIRT is by sending an email to the following address: csirt@cybercircle.eu.

Cyber security experts can be contacted at this email address during hours of operation. We encourage our constituents to use PGP encryption when sending any sensitive information to CYBER CIRCLE CSIRT, to ensure integrity and confidentiality.

CYBER CIRCLE CSIRT's hours of operation are usually restricted to regular Latvian business hours (Monday to Friday 07:00 to 19:00). Outside working days/hours we may operate in case of an emergency only.

3. Charter

3.1. Mission Statement

The mission of CYBER CIRCLE CSIRT is to coordinate and investigate IT security incident response for the Cyber Circle customers.

3.2. Constituency

CYBER CIRCLE CSIRT constituency are the customers of company SIA "CYBER CIRCLE".

3.3. Sponsorship and/or Affiliation

CYBER CIRCLE CSIRT is affiliated to company SIA "CYBER CIRCLE".

3.4. Authority

CYBER CIRCLE CSIRT coordinates security incidents and provides services involving our constituency. Authority with each constituent is stipulated in separate contracts.

4. Policies

4.1. Types of Incidents and Level of Support

CYBER CIRCLE CSIRT addresses all types of security incident which occur, or threaten to occur, within its constituency. The level of support given by CYBER CIRCLE CSIRT depends on the severity of the security incident, its impact and the availability of CYBER CIRCLE CSIRT's resources at the time. Specific support details are described in contracts based on needs between CYBER CIRCLE CSIRT and constituency.

4.2. Co-operation, Interaction and Disclosure of Information

The CYBER CIRCLE CSIRT cooperates with other organisations in the field of cyber security. CYBER CIRCLE CSIRT operates according to the Latvian and EU law and regulations.

CYBER CIRCLE CSIRT is a member of TF-CSIRT.

CYBER CIRCLE CSIRT has strong cooperation with CERT.LV – Latvian National CERT and other cyber security organizations in Latvia and Baltics.

Incident-related information, such as names and technical details, is not published without agreement of involved stakeholders. If not agreed otherwise, supplied information is kept confidential. CYBER CIRCLE CSIRT 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.

CYBER CIRCLE CSIRT understands and supports the traffic light protocol (TLP https://www.first.org/tlp).

4.3. Communication and Authentication

The preferred method of communication is email. For the exchange of sensitive information and authenticated communication CYBER CIRCLE CSIRT uses PGP for encrypting and/or signing messages. All sensitive communication to CYBER CIRCLE CSIRT should be encrypted with our public PGP key.

5. Services

CYBER CIRCLE CSIRT provides multiple services which are described below:

5.1. Incident Response

- 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.

Assist in handling the technical and organizational aspects of incidents response. In particular, 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).
- Categorization of the incident-related information (log files, contact information, etc.) with respect to the information disclosure policy.
- Notification of other involved parties on a need-to-know basis, as per the information disclosure policy.

5.1.3. Incident Resolution

- Analysis of compromised systems.
- Elimination of the cause of a security incident (exploited vulnerability) and securing the system from the effects of the incident.

5.2. Reactive Activities

The CYBER CIRCLE CSIRT team provides the following reactive services:

- Forensic analysis
- Incident analysis
- Incident response
- Incident response coordination
- Incident response on site
- Incident response support
- Vulnerability analysis
- Vulnerability response
- Vulnerability response coordination

5.3. Proactive Activities

The CYBER CIRCLE CSIRT team provides the following proactive services:

- Configuration and maintenance of security tools, applications, and infrastructures
- Security Audits or assessments
- Security related information dissemination
- Technology watch
- Trend and neighborhood watch

5.4. Security Quality Management Services

The CYBER CIRCLE CSIRT team provides the following Security Quality Management services:

- Awareness Building
- Education/Training
- Product evaluation or certification
- Risk analysis
- Security consulting

6. Incident reporting Forms

No special forms are needed to report security incidents to CYBER CIRCLE CSIRT. Please report security incidents via encrypted e-mail to csirt@cybercircle.eu with at least the following information:

- Contact details and organizational information.

- IP address(es), fully qualified domain names (FQDN), and any other relevant technical element with associated observation;
- Any relevant information about a threat or an incident related to CYBER CIRCLE CSIRT constituency.

7. Disclaimers

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