RFC-2350

CERT Alior

Document information:

Title:	RFC-2350 CERT Alior
Date of first release:	13.05.2019
Expiration:	This document is valid until superseded by a later version.
Owner:	Alior Bank
Current version:	1.0
Date of publication of the current version:	13.05.2019

1. Document Information

1.1. Date of Last Update

This is version 1.0, released on 13.05.2019.

1.2. Distribution List for Notifications

Currently CERT Alior does not use any distribution lists to notify about changes in this document.

1.3. Locations where this Document May Be Found

The current version of this document can be found at:
https://www.aliorbank.pl/dodatkowe-informacje/bezpieczenstwo/cert-alior.html

1.4. Authenticating this Document

This document has been signed with the PGP key of CERT Alior. The signature can be found at: https://www.aliorbank.pl/dodatkowe-informacje/bezpieczenstwo/cert-alior.html

2. Contact Information

The section describes how to contact CERT Alior.

2.1. Name of the Team

CERT Alior

2.2. Address

CERT Alior
Alior Bank S.A.
Łopuszańska 38 D
02-232 Warszawa
Poland

2.3. Date of Establishment

CERT Alior was established in October 2010

2.4. Time Zone

Central European Time (GMT+0100, GMT+0200 from April to October)

2.5. Telephone Number

+48 22 5552925

2.6. Electronic Mail Address

All incident reports should be sent to cert[at]alior.pl.

2.7. Public Keys and Encryption Information

The public key and its signature can be found on page:
https://www.aliorbank.pl/dodatkowe-informacje/bezpieczenstwo/cert-alior.html

2.8. Team members

Team CERT Alior consists of IT security experts.

2.9. Other Information

More information about CERT Alior can be found at https://www.aliorbank.pl/dodatkowe-informacje/bezpieczenstwo/cert-alior.html

3. Charter

3.1. Mission Statement

The main purpose of the CERT Alior is taking actions to minimize the probability of occurrence of cyber security incidents, as well as minimizing the effect of their occurrence in constituency, in scope of the provided services

3.2. Constituency

CERT Alior provides cybersecurity incident management for Alior Bank S.A., universal bank in Poland, including entities using Bank's network infrastructure and IT systems, as well as users of Bank's service platforms in the scope of provided service

3.3. Sponsorship and affiliations

CERT Alior is operating within Alior Bank S.A.

3.4. Authority

CERT Alior operates under the auspices of, and with authority delegated by the management of Alior Bank.

4. Policies

4.1. Incidents types and Level of Support

CERT Alior is authorized to address all types of computer and network security incidents which might occur, at Alior Bank's constituency (in the scope of services provided).

CERT Alior prioritizes incidents accordingly to its severity, extend and matter. Incidents are handled accordingly to the priority. The level of support provided by CERT Alior will vary, depending on the severity and type of the issue, as well as other circumstances relevant to case.

4.2. Co-operation, Interaction and Disclosure of Information

CERT Alior exchanges all necessary to cooperation information with other CSIRTs, as well as with affected parties' administrators. No personally identifying information (PII) is exchanged, unless explicitly authorized. All sensitive data (such as PII, system configurations, known vulnerabilities with their locations, etc.) are encrypted, if they must be transmitted over unsecured environment.

CERT Alior recognizes and supports Information Sharing Traffic Light Protocol (v1.1). Any communication that comes with tags supported by the TLP will be handled accordingly**.**

4.3. Communication and Authentication

CERT Alior is bound to obey regulations and policies enforced in Poland and EU covering sensitive information handling.

Any e-mail communication should be tagged using TLP standards. Low-sensitivity data can be sent via unencrypted e-mail, however it's not considered secure. PGP encryption is recommended, especially for sensitive data.

5. Services

5.1. Incident Response

For incidents in scope of its constituency, CERT Alior offers wide range of services, including:

5.1.1. Incident Detection and Analysis

- Determining authenticity of the incident
- Determining root cause of the incident
- Defining the adequate response
- Severity assessment
    - Evaluation of potential risk of occurrence of real effects
    - Evaluation of potential scale of incident and resources that might be affected
    - Prioritization of the incident
- Collecting evidence and indicators of compromise
- Malware analysis
- Reverse engineering

5.1.2. Risk mitigation and Recovery Plan

- Preparing post factum remediation strategy
- Preparing recommendations for security improvements to system administrators
- Developing handling procedures for various types of cyber security incidents

5.1.3. Incidents' Assessment

- Corelating incidents based on collected data
- Continuous search for ways to improve teams performance
- Making reports and securing them for future reference

5.2. Incident Prevention

- Vulnerability response coordination
- Collecting data about security threats and known Indicators of Compromise about from various sources
- Observation of current threats in technology and in security
- Developing and improving existing security tools and mechanisms to constantly enhance the level of security

5.3. Proactive Activities

- Co-creating announcements about new threats for its customers
- Trainings and other activities (such as simulations of real incidents) to improve team's performance

6. Incident Reporting

Security incidents should be reported via encrypted e-mail to cert[at]alior.pl.

7. Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, CERT Alior (as well as Alior Bank S.A.) assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.