CSIRT KNF

RFC 2350

1. About this document

This document contains a description of CSIRT KNF according to RFC 23501 . It provides basic information about CSIRT KNF, its roles and responsibilities and channels of communication.

1.1. Date of Last Update

Version 2.0 published on 11/02/2026

1.2. Distribution List for Notifications

There is no distribution list for notifications.

1.3. Locations where this Document May Be Found

The current version of this document is available at:
https://www.knf.gov.pl/knf/pl/komponenty/img/RFC2350.pdf

1.4. Authenticating this Document

This document has been signed with Qualified electronic signature of CSIRT KNF manager.

2. Contact Information

2.1. Name of the team

CSIRT KNF

2.2. Address

Urząd Komisji Nadzoru Finansowego
Piękna 20
00-549 Warszawa
Poland

2.3. Time Zone

Central European Time (GMT+0100, GMT+0200 from last Sunday in March to last Sunday in October)

2.4. Telephone Number

+48 539 147 782

2.5. Electronic Mail Address

csirt@knf.gov.pl

2.6. Other Telecommunication

None

2.7. Public Keys and Encryption Information

User ID: CSIRT <csirt@knf.gov.pl>
Fingerprint: 26E5 232A 090C 5A0C 9C9D 4BD6 5923 A575 44FC ECD9
The current CSIRT KNF key can be found on:
https://www.knf.gov.pl/dla_rynku/CSIRT_KNF/Klucz_PGP

2.8. Team members

CSIRT KNF team consists of IT security experts.

2.9. Other Information

CSIRT KNF utilizes social media and microblogging platforms to disseminate real-time warnings, threat intelligence regarding the financial sector, and updates on the team's activities.

Facebook: CSIRT KNF maintains an official profile for publishing news and alerts for financial service users at: https://www.facebook.com/p/CSIRT-KNF-100065127625555

X: Short messages regarding current events and technical threat alerts (Cyber Threat Intelligence) are posted on the following account: https://x.com/CSIRT_KNF

General information about CSIRT KNF can be found at:
https://www.knf.gov.pl/dla_rynku/CSIRT_KNF

The csirt@knf.gov.pl mailbox is monitored by the CSIRT KNF team. All incident notifications, threat intelligence reports, and operational queries are processed according to internal CSIRT KNF incident handling protocols. Any incident-related communications received via other functional or departmental mailboxes will be promptly redirected to the primary CSIRT address

3. Charter

3.1. Mission Statement

CSIRT KNF has been created for polish financial sector especially for providers of essential services. The main purpose of the CSIRT KNF team is supporting providers of essential financial services during incident handling.

3.2. Constituency

The constituency of CSIRT KNF consists of entities supervised by the Polish Financial Supervision Authority (KNF), including entities defined in the Act of 5 July 2018 on the National Cybersecurity System (UKSC) and financial entities within the scope of the DORA Regulation (Digital Operational Resilience Act).

3.3. Sponsorship and/or Affiliation

CSIRT KNF team is part of The Polish Financial Supervision Authority (UKNF) which is the financial regulatory authority for Poland.

3.4. Authority

The Act of 5 July 2018 on the National Cybersecurity System (KSC) defines the competencies of the Polish Financial Supervision Authority (UKNF) as the competent authority for cybersecurity in the financial sector.

The Regulation (EU) 2022/2554 (DORA) further establishes the UKNF's role in overseeing the digital operational resilience of financial entities, including incident reporting and oversight.

CSIRT KNF operates within the structures of the UKNF and fulfills the operational tasks of the sectoral CSIRT, specifically addressing:

Incident Coordination: Acting as the central coordinating body for mitigation and recovery efforts during serious, significant, or critical incidents.

Mandatory Reporting and Information Requests: Requesting technical data (logs, malware samples, forensic artifacts) necessary for incident analysis from entities within its constituency.

Sectoral Warning System: Issuing alerts and technical recommendations regarding active threats to maintain sector-wide stability.

Cross-Sectoral and International Liaison: Representing the financial sector in interactions with national-level CSIRTs (CSIRT GOV, CSIRT NASK, CSIRT MON) and international partners during large-scale or trans-border cyber crises

4. Policies

4.1. Types of Incidents and Level of Support

CSIRT KNF is authorized to handle all types of computer security incidents which occur, or threaten to occur, within its constituency, with the scope of its activities specifically defined by the Act of 5 July 2018 on the National Cybersecurity System (UKSC) and Regulation (EU) 2022/2554 (DORA). Incident reports are accepted on a continuous basis via CSIRT KNF’s electronic reporting systems, and the level of support provided depends on the incident's type, its impact on the financial sector's stability, and the current

availability of operational resources. For major or serious incidents classified under DORA or UKSC, acknowledgment of the report and commencement of support activities are performed without delay, while other incidents are acknowledged and supported during business hours.

Incidents are prioritized and classified into several categories, including serious incidents under UKSC that significantly impact the continuity of essential services, and major ICT-related incidents under DORA that adversely affect critical functions of financial entity. The team also coordinates critical incidents involving national or cross-border threats in cooperation with national-level CSIRTs and EU authorities, as well as any other ICT security breaches reported by supervised entities.

While the primary responsibility for incident handling lies with the individual entities, CSIRT KNF provides essential support in the form of cross-sectoral coordination to facilitate information exchange on attack vectors and prevent threat escalation. Furthermore, the team offers technical analysis of provided artifacts and malware samples, alongside the dissemination of relevant Indicators of Compromise (IoCs) through secure communication channels to enhance the overall resilience of the financial sector.

4.2. Co-operation, Interaction and Disclosure of Information

CSIRT KNF exchanges all necessary information with other CSIRTs, entities within the Polish national cybersecurity system, and financial sector participants. The team operates as a trusted hub for the dissemination of technical information regarding threats, attack vectors, and vulnerabilities, ensuring that sensitive data is shared only with authorized parties. No personal data or sensitive business information is exchanged unless explicitly authorized by the reporting entity or required by applicable laws, such as the Act on the National Cybersecurity System (UKSC) or the DORA Regulation.

CSIRT KNF strictly adheres to the FIRST Information Sharing Traffic Light Protocol (TLP 2.0). All communications tagged with TLP:RED, TLP:AMBER, TLP:GREEN, or TLP:CLEAR are handled with the highest level of care and in accordance with the protocol's requirements to ensure appropriate information protection and distribution. Any incoming communication containing TLP tags is treated as a binding instruction for information handling.

All sensitive data, including personal data, system configurations, and specific vulnerability details, is encrypted when transmitted over unsecured networks. CSIRT KNF encourages its constituency and partners to use PGP encryption for all sensitive email communication, utilizing the public key specified in section 2.7 of this document.

4.3. Communication and Authentication

CSIRT KNF requires the use of PGP encryption for the exchange of any confidential or sensitive information via email. For financial entities, the DORA Incident Handling System (SOID) is the primary and designated secure channel for reporting and managing major incidents. Reports regarding serious incidents under the UKSC Act, as well as any other sensitive communications, should be transmitted via email encrypted with the team's public PGP key. While unencrypted communication may be used for initial notifications and low-sensitivity data, it is not considered a secure medium.

To ensure the reliability of shared information, CSIRT KNF verifies the identity of reporting parties through established trust networks within the national cybersecurity system or direct technical validation. The team strongly encourages the use of digital signatures to maintain high assurance levels in all formal communications.

5. Services

CSIRT KNF performs the tasks of a sectoral CSIRT in accordance with Art. 44 of the Act on the National Cybersecurity System (UKSC). The service model is aligned with the FIRST CSIRT Services Framework.

5.1. Prevention and awarness

CSIRT KNF focuses on minimizing incident risks through proactive measures:

- Alerts and Announcements: Publishing information on critical software vulnerabilities and targeted cyber-attack campaigns (Threat Intelligence).
- IoC Distribution: Collecting and sharing Indicators of Compromise (IoCs) via secure channels to enable automated defense mechanisms.
- Awareness Building: Initiatives aimed at increasing cybersecurity competence within the constituency.

5.2. Incident Handling

The core operational service of CSIRT KNF is the coordination and support of incident response reported by its constituency. This process is performed without delay and includes:

- Incident Triage: Immediate confirmation of reports and assessment against UKSC and DORA reporting thresholds.
- Incident Analysis: Providing technical assistance to identify attack vectors and analyzing submitted artifacts, logs, and malware samples.
- Incident Coordination: Acting as a trusted hub for technical information exchange between the reporting entity, other CSIRT/CERT teams, technology vendors, and law enforcement.
- Incident Response Support: Providing actionable technical advice to mitigate impact and prevent cross-sectoral escalation.
- Post-Incident Activity: Analyzing "Lessons Learned" from handled incidents to enhance the overall digital resilience of the financial sector.

5.3. Knowledge Management

- Trend Analysis: Monitoring incident data to identify long-term threat patterns targeting the Polish financial market.
- DORA Resilience Support: Consolidating ICT-related incident data to strengthen the digital operational resilience of financial entities.

6. Incident Reporting

The method for reporting incidents to CSIRT KNF depends on the legal classification and the reporting entity. The use of PGP encryption is highly recommended for sensitive information.

Serious Incidents (under UKSC)
Entities obligated under the Act on the National Cybersecurity System (e.g., Essential Service Operators) should:

1. Complete the dedicated CSIRT KNF Incident Reporting Form
2. Send the completed form to: csirt@knf.gov.pl

The form is available at:
https://www.knf.gov.pl/knf/pl/komponenty/img/CSIRT_KNF_Formularz_zglaszania_incydentow_69998.pdf

DORA Incidents
Financial entities subject to the DORA Regulation are required to report major ICT-related incidents and may voluntarily notify the authority of significant cyber threats using the dedicated DORA Incident Handling System (SOID).
This system, accessible at https://csirt.knf.gov.pl, serves as the primary technical channel for such reports, ensuring the security and authenticity of shared information within the framework of digital operational resilience oversight.

Other Incidents:
Other security incidents, including those reported by third parties or entities falling outside the mandatory reporting scopes of DORA and UKSC, as well as general threat intelligence, should be reported via email to csirt@knf.gov.pl. This channel is also available for reporting vulnerabilities or security issues identified in financial systems by external observers. In cases where the information is confidential or sensitive, encryption using the CSIRT KNF public PGP key is required to ensure data protection.

7. Disclaimers

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

Karol Sławomir Paciorek

Elektronicznie podpisany przez Karol Sławomir Paciorek
Data: 2026.02.11 11:39:06 +01'00'