RFC 2350

1 Document information

This document contains a description of KBC Group CERT as implemented by RFC 2350[1]. It provides basic information about KBC Group CERT, its channels of communication, its roles and responsibilities.

1.1 Date of Last Update

Version 2, created 9-MAR-2020.

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 KBC Group CERT's website: URL:

https://www.kbc.com/en/security

1.4 Authenticating this Document

A signed version of this document can be received on request.

1.5 Document Identification

Title: 'RFC2350-KBC Group CERT-EN'
Version: 2
Document Date: 9 MAR 2020
Expiration: this document is valid until superseded by a later version

2 Contact Information

2.1 Name of the Team

KBC Group CERT

2.2 Address

KBC Group NV IRX/CERT
Havenlaan 2
1080 Brussels
Belgium

2.3 Time Zone

[1] http://www.ietf.org/rfc/rfc2350.txt

CET (Central European Time zone) (GMT+1)

2.4 Telephone Number

+32 2 429 34 14 (during Belgian business hours).

2.5 Facsimile Number

None available.

2.6 Electronic Mail Address

If you need to notify us about an information security incident or a cyber-threat targeting or involving KBC Group, please contact us at:
cert(at)kbc.com

2.7 Other Telecommunication

None.

2.8 Public Keys and Encryption Information

PGP key:

- ID: **0xBDC5EBF7**
- Fingerprint: **75FF 9C70 F60D 7803 0EBF 77BA 8765 7274 BDC5 EBF7**

The key can be retrieved from one of the usual public key servers such as http://pgp.mit.edu/.

2.9 Team Members

A full list of KBC Group CERT team members is not publicly available. Team members will identify themselves to the reporting party with their full name in an official communication regarding an incident.

2.10 Other Information

2.11 Points of Customer Contact

The preferred method to contact KBC Group CERT is to send an e-mail to the address cert(at)kbc.com which is monitored during hours of operation.

Urgent cases can be reported by phone on +32 2 429 34 14 .

Days/Hours of Operation are restricted to regular Belgian business hours
(Monday to Friday 08:00 to 18:00).

3 Charter

3.1 Mission Statement

Our mission is to protect the KBC Group Business Assets against Cyber Threats by:

- Actively supporting our local Business Unit CSIRTs to keep their Cyber Capabilities on due level
- Ensuring Objective and Tailor-made Reporting on Cyber Risk to KBC Group Executive Committee on the different KBC Business entities
- Mitigating the impact of Cyber incidents by ensuring Professional Incident Response coordination and leveraging the internal and external Cyber Risk Community

3.2 Constituency

The KBC Group is a Financial institution. It consists of organizations active in Banking, Insurance and related services as there are Leasing, Trade Finance and Asset Management.

The KBC Group CERT constituencies consists of all entities of KBC Group, their employees and their customers when using applications of the Group.

The constituencies are located mainly in the following countries: Belgium, Czech Republic, Hungary Slovakia, Bulgaria, Ireland, China, France, Germany, Luxembourg, Netherlands, Poland, Singapore, UK and USA.

3.3 Sponsoring Organization/Affiliation

KBC Group CERT is hosted in the KBC Group NV. It maintains contacts with various national and international CSIRT and CERT teams according to its needs and the information exchange culture that it values.

3.4 Authority

KBC Group CERT operates under the authority of KBC Group Executive Committee.

4 Policies

4.1 Types of Incidents and Level of Support

KBC Group CERT is authorized to handle all types of Cyber incidents that would hamper the entities of KBC Group.

The level of support and coordination to the local CSIRTs of the KBC Business entities will vary depending on the severity of the security incident or issue, its potential or assessed impact.

4.2 Co-operation, Interaction and Disclosure of Information

KBC Group CERT highly regards the importance of operational coordination and information sharing between CERTs, CSIRTs, SOCs and similar bodies.

KBC Group CERT operates under KBC rules which are based on (European) privacy guidelines (95/46/EG) and Belgian privacy law.

KBC Group CERT will use the information you provide to help solve security incidents. Information will only be distributed further to other teams and members by default on a need-to-know base, and preferably in an anonymized way, unless otherwise stipulated according to the ISTLP (Information Sharing Traffic Light Protocol) version 1.1[2].

KBC Group CERT also complies with the CCoP (CSIRT Code of Practice) version 2.1[3].

4.3 Communication and Authentication

The preferred method of communication is via e-mail. When the content is sensitive or requires authentication, the KBC Group CERT PGP key is used for signing e-mail messages. All sensitive communication to KBC Group CERT should be encrypted with the team's PGP key.

5 Services

5.1 Service offering selection

As KBC Group CERT is supporting our local CSIRTs, the service offering is built around 4 key domains:

- Crisis & Incident Management
- Cyber Threat Intelligence
- Resilience and Readiness testing
- Training and Awareness

The service offering is delivered by our team, subcontracted to our local CSIRTS or 3rd party service providers.

5.2 Reactive services

KBC Group CERT provides

- Alerts and warnings
- Artifact analysis
- Forensic analysis
- Incident response support
- Incident response on-site
- Incident response coordination

[2] https://www.trusted-introducer.org/ISTLPv11.pdf
[3] https://www.trusted-introducer.org/CCoPv21.pdf

- Vulnerability analysis
- Vulnerability response coordination

5.3 Proactive services

KBC Group CERT provides

- Announcements
- Security audits or assessments
- Security-related information dissemination
- Technology watch
- Trend and neighborhood watch

5.4 Security quality management services

KBC Group CERT performs

- Awareness building
- Cyber resilience measurement
- Education and training

6 Incident Reporting Forms

No local form has been developed yet to report incidents to KBC Group CERT.

In case of emergency or crisis, please provide to KBC Group CERT at least the following information:

- contact details and organizational information – name of person and organization name and address;
- email address, telephone number;
- IP address(es), FQDN(s), and any other relevant technical element with associated observation;
- scanning results (if any) - an extract from the log showing the problem;
- in case you wish to forward any emails to KBC Group CERT, please include all email headers, body and any attachments if possible and as permitted by the regulations, policies and legislation under which you operate.

7 Disclaimers

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