CERT Crédit Mutuel Euro-Information

RFC 2350

About this document

This document contains the description of the CERT Crédit Mutuel Euro-Information as with RFC 2350[1]. The information present in this document is classified *TLP: WHITE*.

TLP: WHITE: The information can be shared publicly and is subject to standard copyright rules.

Date of last update

The first version of this document (1.0) was written in March 2018.

This is version 4.2, published on June 2022.

A detailed history is available at the end of this document.

Distribution list for notifications

Currently, CERT Crédit Mutuel Euro-Information does not use any distribution list to notify about modifications of this document.

Document's Location

The latest version of this document can be found at: **https://www.creditmutuel.fr/en/cert.html**

Contact information

Name of the team

CERT Crédit Mutuel Euro-Information

Short name of the team

CERT CM EI

Address

CERT Crédit Mutuel Euro-Information – Euro Information, 4 Rue Frédéric-Guillaume Raiffeisen - 67000 Strasbourg - France

Time zone

Paris - CET – Central European Time / HNEC - Heure normale d'Europe centrale / UTC +1

Telephone number

+33 3 88 14 60 01, available 24h/24

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

Electronic mail address

Security Incidents should be addressed at the following e-mail: **cert@creditmutuel.fr**

Public keys and other encryption information

PGP is used for communication between the CERT CM EI and its external partners.

The public key of the CERT CM EI is available at the following address
https://www.creditmutuel.fr/en/cert.html

Identifier: 0x4CE11A39

Fingerprint: BB5B 009C 0D91 8C60 DEC4 5108 2A51 9B02 4CE1 1A39

This key can also be downloaded at: **http://pgp.mit.edu/**

It is used for any information that requires secure transmission.

Other means of communication

Currently, there are no other ways to contact the CERT Crédit Mutuel Euro-Information.

Team members

The team is based on security analysts from Euro-Information.

Other information

All Information about the CERT Crédit Mutuel Euro-Information are available at:
https://www.creditmutuel.fr/en/cert.html

Points of contact

The primary mean of contact for incident reporting is by email at the following address:
cert@creditmutuel.fr

We intervene mostly on office hours: 08am-06pm (Paris - CET – Central European Time)

In case of an emergency, the phone number is reachable 24/7. Security teams on duty will decide to directly manage the issue or not.

Charter

Mission statement

The missions of the CERT Crédit Mutuel Euro-Information are:

- Coordinating in a centralized manner the resolution of security incidents in its constituency
- Analyzing the incidents and threats linked with cybercrime and proposing action plans for minimizing risks
- Performing continuous security watch and monitoring security trends which can threaten the Group
- Communicating with other security communities outside of the Group

Constituency

CERT Crédit Mutuel Euro-Information acts when an incident is linked with the information system of Euro-information. That include 16 groups of Crédit Mutuel (Crédit Mutuel Centre Est Europe, Sud-Est, Île-de-France, Savoie-Mont Blanc, Midi-Atlantique, Loire-Atlantique et Centre Ouest, Centre, Normandie, Dauphiné-

Vivarais, Méditerranéen, Anjou, Massif Central, Antilles-Guyane et Nord Europe, Crédit Mutuel Maine-Anjou, Basse-Normandie and Crédit Mutuel Océan), all the CIC Banks and all the subsidiaries linked to financial, technologies, insurance, real estate, consumer credit, private bank and financing.

Sponsorship and/or Affiliation

CERT Crédit Mutuel Euro-Information and SOC Euro-Information are part of the "Detection and security incident response" domain. The domain manager is also the head of CERT Crédit Mutuel Euro-Information.

He acts directly under the Euro-Information CEO's authority or, by delegation, the Deputy Chief executive officer and the Euro-information Operational Committee. That implies that both SOC and CERT CM EI are independant from the others teams according to best practices.

CERT Crédit Mutuel Euro-Information works closely with the "Crédit Mutuel Alliance Fédérale" CISO and their teams.

It participates in the "Operational Steering Group" of the ISMS of Euro-Information.

CERT Crédit Mutuel Euro-Information is a member of the CECyF since 2018.
(**https://www.cecyf.fr/membres/**).

CERT Crédit Mutuel Euro-Information is a member of the InterCERT-Fr since 2019.
(**https://cert.ssi.gouv.fr/csirt/intercert-fr/**)

Authority

CERT Crédit Mutuel Euro-Information acts under the authority of Euro-Information CEO or, by delegation, the Deputy Chief executive officer and the Euro-information Operational Committee.

Policies

Types of incidents and level of support

The CERT Crédit Mutuel Euro-Information intervenes on all security incidents which occur in its constituency networks.

The level of intervention depends on the type and severity of the incident. Where it is possible, the most critical security incidents will be taken into account within 15 minutes upon reception.

Co-operation, interaction and disclosure of information

The CERT Crédit Mutuel Euro-Information shares all necessary technical information with other security communities. No specific data to the Group or personal data are shared without the explicit consent of authorized and affected persons.

Information shared with other security communities is classified using the TLP protocol (Traffic Light Protocol):

- Information shared under the TLP:RED protocol is restricted to participants only,
- Information shared under the TLP:AMBER protocol is restricted to participants' organizations,
- Information shared under the TLP:GREEN protocol is restricted to the community.
- Information shared under the TLP:WHITE procotol can be freely shared, as long as its diffusion is not illegal.

Communication and authentication

Phone communications carried out by the CERT Crédit Mutuel Euro-Information are unencrypted.

By default, sent e-mails are unencrypted. If they contain sensitive information, emails will be sent preferably using PGP as mentioned earlier.

Services

Incident response (Triage, Coordination, Resolution)

The CERT Crédit Mutuel Euro-Information will assist the Group's experts for resolving security incidents by providing assistance with technical and organizational aspects.

Triage

- Investigate whether an incident occurred or not.
- Assess the severity and the perimeter of the security incident.

Coordination

- Determine the initial cause of the incident.
- Contact with involved parties.
- Contact with judicial and regulatory authorities if necessary, in conjunction with dedicated teams.
- Contact with other CSIRTs (Computer Security Incident Response Teams).
- Prepare internal and external communications with dedicated teams.
- Threat Intel sharing for proactive measures.

Resolution

- Follow-up and support for the remediation of security incidents.
- Collect evidence of the incident.

Proactive services

The CERT Crédit Mutuel Euro-Information is in charge of a global security watch for the Group.

The results of this security watch can notably be communicated trough the weekly publication of an internal security newsletter written in French and translated into English, German and Spanish.

The CERT Mutuel Euro-Information gathers intelligence about threats related to Information Security (including Cyber Threat Intelligence).

Incident reporting forms

Currently, there is no notification form to report a security incident. E-mail is the privileged way to warn the CERT Crédit Mutuel Euro-Information.

Disclaimers

The services of the CERT Crédit Mutuel Euro-Information are provided in the most efficient way possible, but despite all the precautions taken, it is possible that some actions are not fully operational to date.

The CERT Crédit Mutuel Euro-Information cannot be held responsible for any errors or omissions, or eventual damages caused by the documents it has produced.

History

- June 21st 2022 : Minor update
- December 31st 2021: Minor update
- January 30th 2020: Minor update
- February 22nd 2019: Minor update
- October 26th 2018: Minor update

- June 04th 2018: Legal review
- May 30th 2018: minor modifications
- March 16th 2018: minor modifications
- February 16th 2018: Document creation