AG2R LA MONDIALE

RFC2350
CERT AG2R LA MONDIALE
(CERT-ALM)

PUBLIC/TLP/WHITE

Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.
TLP: WHITE information may be distributed without restriction, subject to copyright controls.

Contents

1. Document information

This document contains a description of CERT AG2R LA MONDIALE (CERT-ALM) in accordance with RFC 2350. It provides basic information about CERT AG2R LA MONDIALE, its channels of communication, and its roles and responsibilities.

1.1. Date of last update

Version 1.0, published on 2020-12-01

1.2. Distribution list for notifications

Changes to this document are notified by email to:

- InterCERT-FR / network of French CSIRTs - www.cert.ssi.gouv.fr/csirt/intercert-fr
- ENISA and CSIRTs Network members - www.enisa.europa.eu
- Trusted Introducer service - www.trusted-introducer.org
- FIRST organisation - www.first.org

Please send questions about updates to CERT-ALM team email address: BG_CERT[at]ag2rlamondiale.fr

1.3. Locations where this document may be found

The current and latest version of this document is available on our website at: https://www.ag2rlamondiale.fr/rfc2350-cert-ag2r-la-mondiale

1.4. Authenticating this document

This document has been signed wit the PGP key of CERT-ALM. The PGP public key, ID and fingerprint are available in part 2.8 and on our website at: https://www.ag2rlamondiale.fr/rfc2350-cert-ag2r-la-mondiale

1.5. Document identification

Title: “RFC2350 CERT AG2R LA MONDIALE”
Version: 1.0
Document date: 2020-12-01
Expiration: this document is valid until superseded by a later version

2. Contact information

2.1. Name of the team

Official name : CERT AG2R LA MONDIALE
Short name : CERT-ALM

2.2. Address

AG2R La Mondiale
DRO/SSI/CERT-ALM
154 rue Anatole France
92300 Levallois Perret, France

2.3. Time zone

CET/CEST

2.4. Telephone number

+33141051886 (French 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 AG2R La Mondiale, please contact us at: BG_CERT[at]ag2rlamondiale.fr

2.7. Other telecommunication

None.

2.8. Public keys and encryption information

CERT-ALM has a PGP key:

- ID: 50C1 DFA3 0BE3 4B15
- Fingerprint: CFC4 0D8D 9F97 C692 7F18 72B4 50C1 DFA3 0BE3 4B15
- The public key can be retrieved from one of the usual public key servers.

The key shall be used whenever information must be sent to CERT-ALM in a secure manner.

2.9. Team members

The teams consists of IT security analysts. The list of the CERT-ALM's team members is not publicly available. The identity of CERT-ALM's team members might be divulged on a case by case basis according to the need to know restrictions

2.10. Points of customer contact

The preferred method to contact CERT AG2R LA MONDIALE is to send an email to the following address: BG_CERT[at]ag2rlamondiale.fr
A duty security analyst can be contacted at this email address during hours of operation.
If necessary, urgent cases can be reported by phone (+33141051886) during French business hours.
CERT-ALM's hours of operation are usually restricted to regular French business hours (Monday to Friday 09:00 to 18:00).

3. Charter

3.1. Mission statement

CERT-ALM's mission is to coordinate and investigate IT security incident response for the Group AG2R La Mondiale. CERT-ALM will investigate any security incident that may involve a AG2R La Mondiale Group subsidiarie or AG2R La Mondiale as a source or target of an attack or any cyber-threat.
CERT-ALM will operate according to the following key values:

- Highest standards of ethical integrity;
- Effective responsiveness in case of incidents and emergencies and maximum commitment to resolve the issues;
- Fostering information exchange between AG2R La Mondiale and its peers on a need-to-know basis.

3.2. Constituency

CERT-ALM's constituency is composed of all the elements of AG2R La Mondiale's Information System: its users, its systems, its applications and its networks.

3.3. Affiliation

CERT-ALM is affiliated to AG2R La Mondiale. 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

CERT-ALM operates under the authority of the AG2R La Mondiale's Director General.

4. Policies

4.1. Types of incidents and level of support

CERT-ALM is authorized to handle all types of cyberattacks that would hamper the integrity of AG2R La Monidale's IT assets or harm its interests.
Depending on the security incident's type, CERT-ALM will gradually roll out its services which include incident response and digital forensics.
The level of support given by CERT-ALM will vary depending on the severity of the security incident or issue, its potential or assessed impact and the available CERT-ALM's resources at the time.

4.2. Co-operation, interaction and disclosuer of information

CERT-ALM highly considers the paramount importance of operational coordination and information sharing between CERTs, CSIRTs, SOCs and as well as with other affected parties if they are involved in the incident or incident response process.
No incident or vulnerability related information will be given to other persons. French law enforcement personnel requesting information in the course of a criminal investigation will be given the requested information within the limits of the court order and the criminal investigation, if they present a valid court order from a French court.

4.3. Communication and authentication

All e-mails sent to CERT-ALM should be signed using PGP. All e-mails containing confidential information should be encrypted and signed using PGP. Information received in encrypted form should not be stored permanently in unencrypted form.

For other communication, a phone call, postal service, or unencrypted e-mail may be used. CERT-ALM supports the Information Sharing Traffic Light Protocol (TLP).

5. Services

5.1. Incident Response

CERT-ALM offers the following services :

- Incident triage (report assessment ans verification) and analysis,
- incident categorization and incident response coordination,
- incident response support, technical assistance, eradication et recovery.
- technical crisis unit in case of cyberattacks,
- vulnerability response coordination,

- evidence collection and digital forensic.

5.2. Proactive Activities, prevention

CERT-ALM offers the following services :

- Cyber Threat Intelligence
- research and developpement
- education and training
- security auditing
- security awareness
- Cyberattacks crisis exercice

6. Incident reporting forms

No local form has been developed to report incidents to CERT-ALM.
In case of emergency or crisis, please provide at least the following information:

- contact details and organizational information – name of person and organization name and address, email address, telephone number;
- incident date and time (including time zone);
- IP address(es), ports, protocols, FQDN(s), hash of files, 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 CERT-ALM, please include all original email or headers, body and any attachments if possible and as permitted by the regulations, policies and legislation under which you operate.

7. Disclaimers

This document is provided 'as is' without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

If you notice any mistakes within this document, please send a message to us by e-mail. We will try to resolve such issues as soon as possible.