

ARIANEGROUP CSIRT RFC2350 Description

Date : 2021-04-20	Author : ArianeGroup SAS

Document Revision History

Version	Date	Description of change	Person
1.0	09/07/2020	First version published	Head of Cyberdefense
1.1	20/04/2021	Change short name for CSIRT-AGH Change public key	Head of Cyberdefense

Table of contents

1.	DOCUMENT INFORMATION	4
1.1.	Date of last Update.....	4
1.2.	Distribution list for notifications	4
2.	CONTACT INFORMATION.....	5
2.1.	Name of the Team	5
2.2.	Address.....	5
2.3.	Timezone	5
2.4.	Telephone Number.....	5
2.5.	Fax number.....	5
2.6.	Other Telecommunication	5
2.7.	Electronic Mail Address.....	5
2.8.	Public Keys and Encryption	5
2.9.	Team members.....	5
2.10.	Other information.....	6
2.11.	Point of contact.....	6
3.	CHARTER	7
3.1.	Mission statement.....	7
3.2.	Constituency	7
3.3.	Sponsorship and/or Affiliation	7
3.4.	Authority.....	7
4.	POLICIES	8
4.1.	Types of incidents and Level of support	8
4.2.	Co-operation, interaction and Disclosure of Information.....	8
4.3.	Communication and Authentication	8
5.	SERVICES.....	9
5.1.	Incident response	9
5.2.	Incident triage.....	9
5.3.	Incident coordination.....	9
5.4.	Incident resolution	9
5.5.	Proactive activities.....	9
6.	INCIDENT REPORTING FORMS	10
7.	DISCLAIMERS	11

1. DOCUMENT INFORMATION

This document contains a description of ArianeGroup CSIRT in accordance with RFC 2350 specification. It provides basic information about ArianeGroup CSIRT, describes its responsibilities and services offered.

1.1. Date of last Update

Version 1.1 released on 2021-04-20

1.2. Distribution list for notifications

Not applicable

2. CONTACT INFORMATION

2.1. Name of the Team

Official name:

ArianeGroup Computer Security Incident Response Team

Short name:

CSIRT-AGH

2.2. Address

CSIRT-AGH
7 QUAI ANDRE CITROEN
75015 PARIS
FRANCE

2.3. Timezone

Time zone is CET/CEST: Europe/Paris (GMT+01:00, and GMT+02:00 on DST)

2.4. Telephone Number

Left intentionally blank

2.5. Fax number

Left intentionally blank

2.6. Other Telecommunication

Not applicable

2.7. Electronic Mail Address

Please send incident reports related to ArianeGroup to csirt@ariane.group

2.8. Public Keys and Encryption

User ID: CSIRT-AGH (CSIRT ArianeGroup) <csirt@ariane.group>
Key ID: 0xE5115F62
Key type: RSA
Key size: 4096 Expires: never
Fingerprint: FFA033B89B72F26F3CCCCE9E1AE1EB63E5115F62

2.9. Team members

The ArianeGroup CSIRT Team is composed of operational security specialists from ArianeGroup Cyberdefense department.

2.10. Other information

Not applicable

2.11. Point of contact

The only method to contact us is via e-mail at: csirt@ariane.group

ArianeGroup CSIRT operates during regular business hours.

3. CHARTER

3.1. Mission statement

The ArianeGroup CSIRT's activities are non-commercial.

The mandate of ArianeGroup CSIRT is to:

- Investigate, respond and coordinate cybersecurity incident which can affect ArianeGroup's asset and employees, according to the laws and regulations that may apply.
- Manage cybersecurity risks by providing cyber threat intelligence to the whole ArianeGroup and subsidiaries

3.2. Constituency

The CSIRT-AGH constituency is composed of ArianeGroup and all its subsidiaries.

3.3. Sponsorship and/or Affiliation

The CSIRT-AGH is a private CSIRT in the aerospace sector. ArianeGroup SAS owns, operates and finances it.

3.4. Authority

ArianeGroup CSIRT operates under the auspices, and the authority delegated by the ArianeGroup Head of Cyberdefense (CISO), Valérie Levacque. It is responsible for coordinating the incident response and threat prevention across all ArianeGroup SAS perimeters.

4. POLICIES

4.1. Types of incidents and Level of support

ArianeGroup CSIRT is authorized to address all types of computer security incident which occur, or threaten to occur within its constituencies.

The level of support given by ArianeGroup CSIRT will vary depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected, and the ArianeGroup CSIRT's resources at the time.

ArianeGroup CSIRT's resources will be assigned by priorities, listed in decreasing order:

- Incident response and remediation
- Threat Intelligence analysis and sharing

4.2. Co-operation, interaction and Disclosure of Information

ArianeGroup CSIRT is able to share non-restricted information with other parties, especially CSIRTs community. No information can be published without agreement of the concerned parties. If not agreed otherwise, supplied information is kept confidential. Only data that is required to resolve from a specific incident are disclosed to concerned parties (need to know principle). ArianeGroup CSIRT provides means to support confidentiality and integrity of data that is submitted to or disclosed by ArianeGroup CSIRT.

ArianeGroup CSIRT respects the Information Sharing Traffic Light Protocol (TLP) that comes in with the tags WHITE, GREEN, AMBER or RED as described by the FIRST definitions at: www.first.org/tlp

4.3. Communication and Authentication

The only method of communication is e-mail. ArianeGroup CSIRT supports PGP for encrypted e-mails. All sensitive information should be sent by encrypted e-mail. The details of the current ArianeGroup CSIRT Public PGP key can be found in section 2.8.

5. **SERVICES**

5.1. **Incident response**

ArianeGroup CSIRT handles incident response for ArianeGroup and all its subsidiaries.

5.2. **Incident triage**

- Assessment of the severity of the incident.
- If required the incident will be escalated to the General Management

5.3. **Incident coordination**

- Manage the cyber crisis cell if needed
- Notification of other involved parties on a need-to-know basis, as per the information disclosure policy

5.4. **Incident resolution**

- Manage the incident resolution
- Assist system and network administrators in handling the technical and organizational aspects of incidents

5.5. **Proactive activities**

- Devices and network monitoring
- Threat hunting
- Threat Intelligence
- Sharing information with the CSIRT community and constituency

6. INCIDENT REPORTING FORMS

There are no reporting forms available.

Please send e-mail to csirt@ariane.group and report us any relevant information about the incident. Sensitive information should be sent by encrypted e-mail.

7. DISCLAIMERS

While every precaution will be taken in the redaction of this document, ArianeGroup SAS assumes no responsibility for errors or omissions, or for damage resulting from the use of the information contained within.

If you find any mistakes within this document please send us an e-mail at: csirt@ariane.group