RFC 2350

AMADEUS CERT (1A-CERT)

LEG-SEC-GSO

Last update: 19/03/2025

Table of Contents

Document control

Security level	Public | TLP:WHITE			
Company	Amadeus IT Group SA			
Department	LEG-SEC-GSO			
Author	Nicolas VEYS			
Reviewed by	Daniel MORELAND		Date	[dd/mm/yyyy]
Approved by	Alain SIMON		Date	30/Mar/2020
Version	Date	Change	Comment	By
1.0	29/Mar/2020		Initial	N. VEYS
1.1	25/Jan/2021	OTH > DMO		N. VEYS
1.2	19/Mar/2025	New PGP & template		K. BOUILLET

1.Documentation Information

This document contains a description of Amadeus CERT in accordance to RFC 2350.

It provides basic information about the CERT unit and describes its responsibilities and services it offers.

1.1. Date of Last Update

Version 1.1, published on 25-January-2021.

1.2. Distribution List for Notification

There is no distribution list for notification.

1.3. Locations where this Document May Be Found

The current and latest version of this document is available on AMADEUS corporate public website at:

https://amadeus.com/en/policies/security-amadeus-cert-rfc2350

1.4. Authenticating this Document

This document can be retrieved from our public webserver.

2. Contact Information

2.1. Name of the Team

The full name for the team is **Amadeus CERT** and the team acronym is “**1A-CERT**”.

2.2. Address

Amadeus CERT
485 Route du Pin Montard
06960 Biot
France

2.3. Time Zone

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

2.4. Telephone Number

Amadeus CERT can be reach through Amadeus Main Desk reception during French Office Hours at: **+33 (0)4 92 94 60 00**. Ask for a CERT team. See named contact in section 2.9.

2.5. Facsimile Number

None available

2.6. Other Telecommunication

Not applicable

2.7. Electronic Mail Address

Shall you need to notify us about a potential cyber threat or a cyber security incident involving Amadeus group as source or target, please contact us at cert[at]amadeus.com

Alternative address: soc[at]amadeus.com

2.8. Public Keys and Encryption Information

For secure communication with cert[at]amadeus.com, please encrypt your email using PGP:

- ID: **8B319AB34F17536B**
- Fingerprint: **d7cddaf180ebc525f3f3fe998b319ab34f17536b**
- Download 1A-CERT public key:

  (https://amadeus.com/content/dam/amadeuswebevo/documents/en/security/cert-public-key.pgp)

2.9. Team Members

The list of the 1A-CERT team members is not publicly available but could be divulged on a case by case basis according to the need to know restrictions.

Our Global Security Operations management team is composed of:

Head of Global Security Operations: Olivier THONNARD

- Head of Amadeus CERT Unit: Nicolas VEYS

- Head of Amadeus Global SOC: Horia COASA
- Head of ASOC & Anti-Fraud Unit: Vincent RIGAL

2.10. Other Information

Not applicable

2.11. Points of Customer Contact

1A-CERT prefers to receive incident reports via e-mail at cert[at]amadeus.com. Please use our cryptographic key to ensure integrity and confidentiality.

In case of emergency, please specify the **[URGENT]** tag in the subject field in your e-mail.

1A-CERT's hours of operation are restricted to regular business hours (09:00-18:00 Monday to Friday), all year long. Our Global Security Operations however are running 24/7 all year long.

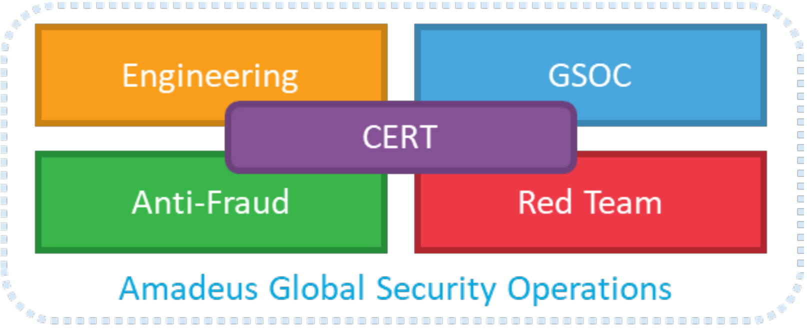
3. Charter

Within this section our mandate is described.

3.1. Mission Statement

Amadeus CERT (1A-CERT) is the team in charge of coordinating the Cyber Threat Intelligence and Cyber Security Incident Response activities between Amadeus Group Internal entities and external entities (Authorities and National CERT, Private & Commercial CERT/CSIRT, Industry ISAC, …). Amadeus CERT Unit is also responsible for developing the group Cyber Defense and Threat Detection Strategy.

The CERT unit is part of the Amadeus Global Security Operations department alongside the Engineering unit, the Global SOC unit, the Anti-Fraud unit and the Offensive Security unit.



3.2. Constituency

Our constituency are composed of AMADEUS IT Group and all subsidiaries.

3.3. Sponsorship and/or Affiliation

The Amadeus CERT (1A-CERT) is a private CERT in the travel, transportation, hospitality and aviation vertical.

1A-CERT is owned, operated and financed by Amadeus IT Group.

1A-CERT is a member of National French Network (InterCERT-FR) and wish to be a member of European Network (TF-CSIRT).

1A-CERT requested authorization from Carnegie-Mellon for the usage of CERT Trademark. CERT-CC is not granting license outside the USA for the time being.

3.4. Authority

Amadeus CERT operates under the auspices of, and with the authority delegated by the Chief Information Security Officer (CISO) of Amadeus IT Group and the Director of the Global Security Operations.

4. Policies

This section describes our policies.

4.1. Types of Incidents and Level of Support

1A-CERT addresses all kinds of security incidents which occur, or threaten to occur, within its constituency. The level of support depends on the type and severity of the given security incident, the amount of affected entities within our constituency, and our resources at the time. Usually our first response comes on the same working day during working hours, if not it will be on the following working day.

Note that no direct support is given to end users; they are expected to contact their Service Desk or Local IT Managers, Security Site Managers for assistance.

4.2. Co-operation, Interaction and Disclosure of Information

1A-CERT will exchange all necessary information with other CERT, CSIRT or ISAC 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

The preferred method of communication is email.

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. 1A-CERT supports the Information Sharing Traffic Light Protocol (TLP).

5. Services

This section describes the services 1A-CERT offers.

5.1. Proactive Activities

The team offers the following services:

- Cyber Threat Monitoring & Threat Notification (Advisory, Bulletin)
- Public Digital Footprint Monitoring
- Cyber Threat Hunting & Purple Teaming
- Vulnerability Analysis & Triage. Vulnerability Response Coordination
- Cyber Threat Intelligence Sharing (including provision of IOC and liaison with Engineering unit to enable ad-hoc detection or prevention controls)

5.2. Incident Detection

The team offers the following services:

- Incident detection via the Global SOC unit.

5.3. Fraud Detection

The team offers the following services:

- Fraud detection & analysis via the ASOC & Anti-Fraud unit.

5.4. Incident Response

The team offers the following services:

- Remote and Local Incident response via the Global SOC unit
- Incident response support to Global SOC unit (via sharing of IOC, TTP, and development signatures)
- Incident response coordination between Amadeus Group Internal entities and external entities (Authorities and National CERT, Private & Commercial CERT/CSIRT, Industry ISAC, …) or Customers

5.5. Engineering & Expertise

The team offers the following services:

- Security Orchestration Tooling
- Adversary Emulation Exercise
- Support to SOC onboarding activities
- Cyber Defense & Threat Detection Strategy
- Security Architecture & Technical Studies
- Auditing services
- Merge & Acquisition Assessment

6. Incident Reporting Forms

We do not have an incident reporting form. Please report security incidents via encrypted e-mail to cert[at]amadeus.com.

Incident reports should contain the following information:

- Incident date and time (including time zone)
- Source IPs, ports, and protocols
- Destination IPs, ports, and protocols
- And any relevant information

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.