TLP:CLEAR

RFC 2350

CERT-Equans

TLP:CLEAR

1. DOCUMENT INFORMATION

1.1. ABOUT THIS DOCUMENT

This document contains a description of Equans Computer Emergency Response Team, which will be referred to as CERT-Equans, in accordance with RFC 2350. It provides basic information about the CERT-Equans team, its channels of communication, its roles and responsibilities.

1.2. DATE OF LAST UPDATE

Version 1.1, published on 13th. January 2023.

1.3. LOCATION WHERE THIS DOCUMENT MAY BE FOUND

The current and latest version of this document is available on CERT-Equans website.
Its URL is www.equans.com/cert.

1.4. AUTHENTICATING THIS DOCUMENT

This document has been signed with the PGP key of CERT-Equans.
The public PGP key is available on CERT-Equans website.

1.5. DOCUMENT IDENTIFICATION

Title: RFC 2350 – CERT-Equans
Version: 1.1
Document Date: 2023/13/01
Expiration: this document is valid until it is replaced by a later version.

2. CONTACT INFORMATION

2.1. NAME OF THE TEAM

Full Name: Equans Computer Emergency Response Team
Short Name: CERT-Equans

2.2. ADDRESS

Postal Address: CERT-Equans, 49-51 rue Louis Blanc, 92400 Courbevoie, France.

2.3. TIME ZONE

CET/CEST (UTC +1/UTC +2), Central European Time / Central European Summer Time.

2.4. TELEPHONE NUMBER

The Equans Cyberdefense Team can be reached at all time at: +33 1 73 17 04 00.

2.5. ELECTRONIC EMAIL ADDRESS

CERT-Equans can be reached via cert@equans.com.

2.6. PUBLIC KEYS AND OTHER ENCRYPTION INFORMATION

In order to guarantee the security of communications, the PGP technology is supported. CERT-Equans public PGP key ID is 0xC523CC19. This PGP key is available on the public PGP key servers and in CERT-Equans website. It shall be used to encrypt communication whenever information must be sent to CERT-Equans at cert@equans.com in a secure manner.

2.7. TEAM MEMBERS

CERT-Equans's Team Leader is Leon GUBBELS. The complete list of team members is not published, but consists of Security Analysts and Specialists.

2.8. OTHER INFORMATION

General information about the CERT-Equans can be found at CERT-Equans website: https://www.equans.com/cert.
A French version of this page is available at https://www.equans.com/fr/cert.

2.9. POINT OF COSTUMER CONTACT

The preferred method for contacting CERT-Equans is by mail at: cert@equans.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. An analyst will be assigned during working hours.

3. CHARTER

3.1. MISSION STATEMENT

The CERT-Equans team's activities are non-profit and fully financed by Equans S.A.S.

CERT-Equans is part of the Equans Cyberdefense Team. CERT-Equans is the team in charge of Information Security Incident Management and Vulnerability Management. This covers – but is not limited to – artefact and forensic evidence analysis, information security incident coordination, crisis management support, vulnerability discovery, analysis, coordination and response, external threats, misconfigurations and data leak monitoring.

3.2. CONSTITUENCY

The constituency of CERT-Equans refers to all the legal entities in Equans Group.

3.3. SPONSORSHIP AND/OR AFFILIATION

CERT-Equans is part of Equans S.A.S., a Bouygues Group company.

3.4. AUTHORITY

CERT-Equans operates with authority delegated by Equans S.A.S.

4. POLICIES

4.1. TYPE OF INCIDENT AND LEVEL OF SUPPORT

CERT-Equans manage and address unknown type and critical information security incident which occur or threaten to occur in its constituency. The level of support given by CERT-Equans will vary depending on the severity of the incident, the related Equans Information and Communication Technology (ICT) assets impacted and the CERT-Equans resources at the time.

The services provided by CERT-Equans include:

- Artefact and forensic evidence analysis;
- Information security incident coordination;
- Crisis management support;
- Vulnerability discovery;
- Vulnerability analysis;
- Vulnerability coordination;
- Vulnerability response;
- External threats, misconfigurations and data leak monitoring.

CERT-Equans operates under the current French legal framework.

4.2. CO-OPERATION, INTERACTION AND DISCLOSURE OF INFORMATION

CERT-Equans knows the importance for sharing information with third parties. The "need to know" principle is applied in order to share the necessary amount of information to the restricted people/organizations involved. In addition CERT-Equans respects the Information Sharing Traffic Light Protocol Version 2 (TLP 2.0) that comes with the tags CLEAR, GREEN, AMBER, AMBER+STRICT or RED as described by the FIRST definitions at: www.first.org/tlp/

CERT-Equans can exchange with other entities such as external SOC, CERT and other Cybersecurity teams in order to facilitate information sharing. CERT-Equans dialogs and cooperates with a privilege way with Cybersecurity entities close to their activities.

4.3. COMMUNICATION AND AUTHENTICATION

The preferred way to exchange information and communicate with CERT-Equans is via email. CERT-Equans recommends using cryptographic PGP to communicate securely with them. The TLP tag is also recommended in order to facilitate the initial triage realized by the team.

5. SERVICES

5.1. REACTIVE ACTIVITIES

The team offers the following reactive services:

- Alerts and Warnings;
- Incident Coordination;
- Crisis Management;
- Artifact Handling;
- Vulnerability Response Coordination.

5.2. PROACTIVE ACTIVITIES

The team offers the following proactive services:

- Threat intelligence monitoring (including external threats, misconfigurations and data leak monitoring);
- Vulnerability exposure monitoring;
- IOC sharing.

6. INCIDENT REPORTING

CERT-Equans does not provide any incident reporting form in a public web page. Please report security incidents via encrypted e-mail to cert@equans.com.

Please classify the information using the Traffic Light Protocol. 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. DISCLAIMER

While every precaution will be taken in the preparation of information, notifications and alerts, CERT-Equans assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.