TLP:CLEAR

RFC 2350

CSIRT-Equans

TLP:CLEAR

1. DOCUMENT INFORMATION

1.1. ABOUT THIS DOCUMENT

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

1.2. DATE OF LAST UPDATE

Version 1.3, published on 1st. July 2024.

1.3. LOCATION WHERE THIS DOCUMENT MAY BE FOUND

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

1.4. AUTHENTICATING THIS DOCUMENT

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

1.5. DOCUMENT IDENTIFICATION

Title: RFC 2350 – CSIRT-Equans
Version: 1.3
Document Date: 2024/10/1
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 CSIRT
Short Name: CSIRT-Equans

2.2. ADDRESS

Postal Address: Equans CSIRT, 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 a time at: **+1 361 470 2515**.

2.5. ELECTRONIC EMAIL ADDRESS

CSIRT-Equans can be reached via csirt@equans.com.

2.6. PUBLIC KEYS AND OTHER ENCRYPTION INFORMATION

In order to guarantee the security of communications, the PGP technology is supported.

This PGP key is available on the public PGP key servers and from CSIRT-Equans website.

It shall be used to encrypt communication whenever information must be sent to CSIRT-Equans at csirt@equans.com in a secure manner.

CSIRT-Equans public PGP key ID is 0xDE98A46BB8E11DE0

Fingerprint:6832 6B56 A27A 9225 492B EC66 DE98 A46B B8E1 1DE0

2.7. TEAM MEMBERS

CSIRT-Equans' Team Leader is Alexandre Augagneur. The complete list of team members is not published, but consists of Security Analysts and Specialists.

2.8. OTHER INFORMATION

General information about the CSIRT-Equans can be found at CSIRT-Equans website: https://www.equans.com/csirt.

2.9. POINT OF COSTUMER CONTACT

The preferred method for contacting CSIRT-Equans is by mail at: csirt@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.

3. CHARTER

3.1. MISSION STATEMENT

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

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

3.2. CONSTITUENCY

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

3.3. SPONSORSHIP AND/OR AFFILIATION

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

3.4. AUTHORITY

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

4. POLICIES

4.1. TYPE OF INCIDENT AND LEVEL OF SUPPORT

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

The services[1] provided by CSIRT-Equans include:

- Monitoring and detection ;
- Information security incident analysis
- Artefact and forensic evidence analysis;
- Mitigation and recovery ;
- Information security incident coordination;
- Crisis management support.

CSIRT-Equans operates under the current French legal framework.

4.2. CO-OPERATION, INTERACTION AND DISCLOSURE OF INFORMATION

CSIRT-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 CSIRT-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/

CSIRT-Equans can exchange with other entities such as external SOC, CERT and other Cybersecurity teams in order to facilitate information sharing. CSIRT-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 CSIRT-Equans is via email. CSIRT-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.

[1] As defined by CSIRT Services Framework Version 2.1 (first.org)

5. SERVICES

5.1. INCIDENT RESPONSE

5.1.1. INCIDENT TRIAGE

Incident reported are initially reviewed, categorized, prioritized, and processed by CSIRT-Equans.

5.1.2. INCIDENT COORDINATION

CSIRT-Equans ensures Information security incident coordination and Crisis management support for its constituency and acts as point-of-contact with internal constituency and external partners when needed.

5.1.3. INCIDENT RESOLUTION

The team offers the following reactive services:

- Information security incident analysis ;
- Artefact and forensic evidence analysis ;
- Mitigation and recovery.

5.2. PROACTIVE ACTIVITIES

The team offers the following proactive services:

- Monitoring and detection ;
- Vulnerability Analysis.

6. INCIDENT REPORTING

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

Information must be classified using the Traffic Light Protocol[2]. 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, CSIRT-Equans assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.

End of document

[2] Traffic Light Protocol (TLP) (first.org)