RFC2350

FS-CERT

1. DOCUMENT INFORMATION

1.1. ABOUT THIS DOCUMENT

This document contains a description of Gruppo FS-Computer Emergency Response Team (CERT), (hereinafter referred as to FS-CERT) in according to RFC 2350. It defines the basic information related to FS-CERT, including a brief explanation of the tasks and services offered and contacts to get in touch with us.

1.2. DATE OF LAST UPDATE

Version 1.0, updated on 17/12/2021.

1.3. LOCATIONS WHERE THIS DOCUMENT MAY BE FOUND

The current and latest version of this document is available on FS-CERT website.

Its URL is https://www.fsitaliane.it/content/fsitaliane/en/fs-group/governance/computer-emergency-response-team.html.

1.4. AUTHENTICATING THIS DOCUMEN

This document has been signed with the GPG key of FS-CERT.

The public GPG key is available in FS-CERT website.

1.5. DOCUMENT IDENTIFICATION

Title: FS-CERT-RFC 2350

Version: 1.0.

Document Date: 17/12/2021

Expiration: this document is valid until a later version is issued.

2. CONTACT INFORMATION

2.1. NAME OF THE TEAM

Full Name: Gruppo FS-Computer Emergency Response Team (CERT)

Short Name: FS-CERT

2.2. ADDRESS

Postal Address: Piazza della Croce Rossa 1, 00161 Roma

Time zone: Central European (GMT+0100 and GMT+0200 from the last Sunday of March to the last Sunday of October).

2.3. TELEPHONE NUMBER

Tel: (H24/7 365 day): +393316360190

2.4. ELECTRONIC MAIL ADDRESS

The email csirt@fsitaliane.it is available to contact FS-CERT. All members of FS-CERT team can read the messages sent to this address.

2.5. PUBLIC KEYS AND OTHER ENCRYPTION INFORMATION

In order to guarantee the security of communications the GPG technology is employed. FS-CERT's public GPG key for csirt@fsitaliane.it is available on FS-CERT website.

FS-CERT's Public Key:

- USER-ID: CSIRT FS
- KEY-ID: 1917 D2F6 8A40 456D
- Fingerprint: 3DF0 34BB 0624 7D71 D000 5053 1917 D2F6 8A40 456D

Third parties shall use GPG public key to establish a secure communication with FS-CERT

2.6. TEAM MEMBERS

FS-CERT's Team Leader is the Head of CERT, Riccardo Barrile. The team consists of Stefano Cortellessa, the Deputy Head of CERT, CERT Coordinators and CERT Analysts.

3. OTHER INFORMATION

General information about FS-CERT are available on FS-CERT website: https://www.fsitaliane.it/content/fsitaliane/en/fs-group/governance/computer-emergency-response-team.html.

3.1. POINTS OF CUSTOMER CONTACT

The email address csirt@fsitaliane.it is the preferred method to contact FS-CERT.

The mailbox is monitored 24/7.

The use of GPG is mandatory when confidential or sensitive information are involved.

If for security reasons it is not possible to get in touch with FS-CERT via e-mail, the contact may take place via telephone.

3.2. CHARTER

3.2.1. MISSION STATEMENT

In conjunction with Cyber Security Operation Center (C-SOC) and other relevant structures of the Group, the Computer Emergency Response Team (FS-CERT) provides the entire Ferrovie dello Stato Italiane Group (FS Group) with the Cyber Security Services under its responsibility. The main are listed below:

- protection of information systems and service production infrastructures by means of defining security requirements within ICT projects in compliance with current regulations and best practices, and identifying and deploying appropriate technological security solutions;
- centralized threat detection and incident response with the aim of identifying, containing and mitigating vulnerabilities and cyber attacks targeting the infrastructures and information systems that enable the Group's services, including IT systems for sales and railway traffic, and the SCADA/ICS perimeter;

- conduction of Security Risk Assessment activities of the Group's ICT systems.

Furthermore, CERT is the FS Group's national and international cyber security center of competence, maintaining relationships with institutional CERTs/CSIRTs and national critical infrastructures for knowledge exchange and the study of new techniques to counter cyberattacks.

3.2.2. CONSTITUENCY

The Constituency consists of the entire Ferrovie dello Stato Italiane Group (FS Group). FS-CERT provides the Group's companies - including subsidiaries and their assets - with the whole Cyber Security service portfolio, as established within the service contracts. Furthermore, FS-CERT focuses on protecting and safeguarding the Constituency's business infrastructures and services - as well as the confidentiality, integrity and availability of its information assets - from potential threats within the cyberspace, by preventing, containing and neutralizing malicious events both within the Information Technology (IT) and Operational Technology (OT) environments.

3.2.3. SPONSORSHIP AND/OR AFFILIATION

FS-CERT is affiliated to Ferrovie dello Stato Italiane S.p.A. It maintains contacts with various national and international CERT and CSIRT teams, with FIRST, TFCSIRT, ENISA and Carnegie Mellon University according to its needs and to its culture of information exchange.

3.2.4. AUTHORITY

The establishment of the FS-CERT was mandated on 01/11/2017.

3.3. POLICIES

3.3.1. TYPE OF INCIDENT AND LEVEL OF SUPPORT

FS-CERT manages and addresses information security incidents, which occur or threaten to occur within its constituency. The level of support given by FS-CERT will vary depending on the severity of the information security incident, the assets impacted and the CERT's currently available resources.

3.3.2. CO-OPERATION, INTERACTION AND DISCLOSURE OF INFORMATION

FS-CERT highly values the importance of operational coordination and information sharing among CERTs, CSIRTs, SOCs and similar parties, as well as other organizations, which may aid them in delivering their services or provide other benefits. FS-CERT recognizes and supports ISTLP (Information Sharing Traffic Light Protocol).

3.3.3. COMMUNICATION AND AUTHENTICATION

FS-CERT protects sensitive information in accordance with relevant local regulations and policies. Communication security (which includes both encryption and authentication) is primarily achieved using GPG or any other agreed means, depending on the sensitivity level and context.

4. SERVICE

4.1. INCIDENT MANAGEMENT

The main goal of Incident Management service is the management of cyber incidents detected by the continuous monitoring of security events in order to contain their potential impacts on the internal and external constituency, consisting of national and international institutions and organizations. Incident management process as developed by FS-CERT cover all the following steps:

- Preparedness and prevention;
- Detection;
- Analysis;

- Response;
- Recovery.

4.2. THREAT INTELLIGENCE

FS-CERT researches, analyses and collects potentially useful external information in order to detect emerging advanced cyber threats and identify useful information to prevent their spread within the Group's ICT perimeter.

5. INCIDENT REPORTING FORM

FS-CERT does not provide any incident reporting form in a public web page.
As for FS-CERT's constituency, the incident reporting must follow the internal procedures.

6. DISCLAIMERS

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