e.SNCF SOLUTIONS
DIRECTION CYBERSECURITE

TLP:CLEAR

CERT SNCF

RFC 2350	Version 2.0	25/09/2023

A PROPOS

Ce document contient une description du CERT SNCF selon le document RFC 2350[1].

Il fournit les informations essentielles concernant le CERT SNCF, son rôle, ses responsabilités et ses moyens de communication.

VERSION DE DOCUMENT

La version de ce document est la 2.0, publiée en Septembre 2023.

LISTE DE DISTRIBUTION

Aucune liste de distribution.

LIEU DE PUBLICATION DU DOCUMENT

La version actuelle de ce document peut être consultée sur notre site :

https://www.cert-sncf.fr/CERT-SNCF-RFC2350-FR.pdf

AUTHENTICITE DU DOCUMENT

Les versions anglaise et française de ce document sont signées avec la clé PGP du CERT SNCF.

[1] ietf.org/rfc/rfc2350.txt

CONTACTS

Cette partie décrit les moyens de communication du CERT SNCF.

NOM

CERT SNCF

ADRESSE

CERT SNCF

Département CyberSécurité Opérationnelle

Campus Rimbaud – Bureau D1.002.B

12 rue Jean-Philippe Rameau - CS80001 –

93212 Saint-Denis

FUSEAU HORAIRE

Heure d'été d'Europe centrale ou heure d'Europe centrale (CET ou CEST).

NUMERO DE TELEPHONE

+33 800 00 60 67

AUTRE CANAL DE COMMUNICATION

Message privé via le compte X : https://twitter.com/CertSNCF

Attention : aucune information confidentielle ne doit et ne sera communiquée via X.

ADRESSE DE COURRIER ELECTRONIQUE

cert@sncf.fr

CLE PUBLIQUE ET INFORMATIONS DE CHIFFREMENT

Le CERT SNCF possède une clé publique PGP:

- Utilisateur : cert@sncf.fr
- Identification de la clé : 759E5CDAC4D5555E
- L'empreinte de la clé est : 1E6A918598366CCAB6678702759E5CDAC4D5555E

La clé publique du CERT SNCF se trouve sur le site du CERT SNCF :

https://www.cert-sncf.fr/CERT-SNCF_PUB.asc

COMPOSITION DE L'EQUIPE

L'équipe est constituée d'analystes et d'experts cyber sécurité.

Aucune information nominative relative aux membres du CERT SNCF n'est diffusée dans ce document.

POINTS DE CONTACT

Il est préférable de contacter le CERT SNCF par mail à cert@sncf.fr

En cas d'impossibilité d'envoyer un courrier électronique il est possible de contacter le CERT SNCF par téléphone en journée, du lundi au vendredi de 08h à 18h.

Une astreinte téléphonique 24/7 est assurée par le CERT SNCF.

CHARTE

MISSIONS

Les missions du CERT SNCF sont : la gestion des incidents de cybersécurité ou des incidents liés à de la cyber criminalité, la gestion des vulnérabilités, la fourniture de services d'analyses techniques avancées et de coordination de la réponse dans le cadre d'incident de sécurité ciblant les entités du groupe SNCF. Le CERT SNCF effectue un renseignement sur les menaces cyber, et les recherches proactives de ces menaces sur les systèmes d'informations.

Le CERT SNCF intervient également dans la gestion de Crise cybersécurité du système d'information du groupe SNCF.

CIRCONSCRIPTION

Le CERT SNCF assure ses missions pour l'ensemble des entités du groupe SNCF : les différentes Sociétés Anonymes et l'ensemble des filiales pour lesquelles SNCF est directement ou indirectement actionnaire majoritaire et tel que décrit sur la page de présentation de l'organisation du groupe SNCF https://www.sncf.com.

AFFILIATION

Le CERT SNCF est rattaché à la Direction Cybersécurité - e.SNCF Solutions de la DGA Numérique.

AUTORITE

Le CERT SNCF est soutenu par la SA SNCF et le DG Numérique.

Au titre de ses missions, le CERT SNCF est autorisé à lancer les vérifications techniques sur l'exploitabilité d'une vulnérabilité qui toucherait un élément des systèmes d'informations du groupe SNCF dans le seul objectif d'identifier les systèmes vulnérables et lancer les remédiations dans les meilleurs délais.

Ce pouvoir n'est pas transférable.

Au titre de ses missions, le CERT SNCF est autorisé à coordonner, analyser et contribuer à la résolution de tout incident de cybersécurité qui cible ou pourrait cibler une entité du Groupe SNCF, sans avoir nécessairement été sollicité au préalable par une personne de l'entité concerné.

TYPES D'INCIDENTS ET NIVEAU DE SUPPORT

Le niveau de support offert par le CERT SNCF peut varier en fonction de la catégorie d'un incident, de sa complexité et de sa criticité.

COOPERATION, ECHANGES, ET CONFIDENTIALITE DE L'INFORMATION

Le CERT SNCF échangera, dans la mesure du possible, les informations nécessaires avec les autres CERT/CSIRT susceptibles d'être concernés selon le besoin d'en connaître.

Le CERT SNCF applique le TLP (Traffic Light Protocol) version 2.0 et le PAP (Permissible Actions Protocol) selon la politique de partage appliquée par l'ANSSI[2].

MOYENS DE COMMUNICATION

L'échange d'informations confidentielles par courrier électronique devra être chiffré via PGP.

Même s'il n'est pas considéré comme sûr, un courrier électronique non chiffré sera considéré comme suffisant dans le cadre de transmission d'information non confidentielle.

Concernant le partage de fichier, nous utilisons l'outil LockTransfer (https://www.lockself.com/) qui permet de fournir des liens de partage de fichiers sécurisés à un tier.

[2] Politique de partage et d'utilisation des informations à caractère opérationnel – CERT-FR (ssi.gouv.fr)

MISSIONS

REPONSE AUX INCIDENTS CYBERSECURITE

Dans le cadre de la réponse aux incidents cybersécurité, le CERT SNCF effectue les taches suivantes :

- Triage, qualification et analyse de l'incident
- Coordination de réponse technique lors d'un incident
- Assistance à la remédiation
- Analyses approfondies (forensic)
- Intervention d'urgence pour les incidents les plus critique.

RECHERCHES PROACTIVES

Le CERT SNCF réalise une veille sur les menaces, les vulnérabilités, les scénarios d'attaques et les mesures de sécurité nécessaires pour protéger les systèmes d'information des entités du groupe SNCF.

Ces informations peuvent être échangées avec d'autres CERT/CSIRT dans le respect des pratiques de partage et d'exploitation des informations.

FORMULAIRE DE DECLARATION D'INCIDENT

Le CERT SNCF ne possède pas de formulaire type pour déclarer un incident de sécurité. Merci de signaler l'incident par courrier électronique à l'adresse cert@sncf.fr

AVERTISSEMENTS

Bien que les informations transmises dans le document aient été vérifiées, le CERT SNCF décline toute responsabilité en cas d'erreur ou d'omission ou pour tout préjudice résultant d'informations contenues dans ce document.

En cas d'erreur constatée dans ce document merci de le signaler par mail.