CSIRT CNES

RFC 2350 V1.0

DESCRIPTION DES SERVICES

Thierry
DEMANGEOT

Signature numérique de Thierry DEMANGEOT
Date : 2023.12.08 16:44:48 +01'00'

TLP:CLEAR

CSIRT CNES RFC 2350

Table des matières

CSIRT CNES RFC 2350

1. A propos de ce document

Ce document contient une description du CSIRT CNES répondant aux préconisations de la RFC2350. Il décrit les informations essentielles sur le CSIRT CNES, ses responsabilités et les services fournis.

1.1. Date de dernière mise à jour

V1.0 applicable au 01/01/2024.

1.2. Liste de diffusion des modifications

DIFFUSION	MARQUAGE
InterCERT France	TLP CLEAR
Internet	TLP CLEAR

1.3. Espace de diffusion de ce document

La version courante de ce document est disponible sur le site internet du CSIRT CNES https://csirt.cnes.fr/ < en construction> ou par mail à l'adresse ci-dessous.

1.4. Authenticité de ce document

Ce document a été signé avec Adobe PDF.

CSIRT CNES RFC 2350

2. Information sur le CSIRT

2.1. Nom de l'entité

Nom complet : Cellule de Réponse aux Incidents de Cybersécurité pour le CNES.
Nom abrégé : CSIRT CNES

2.2. Adresse

Centre National d'Etudes Spatiales (CNES)
18 Avenue Edouard Belin
31409 TOULOUSE Cedex 9

2.3. Zone de temps

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

2.4. Numéro de téléphone

+33 7 86 28 47 04

2.5. Numéro de fax

Sans objet

2.6. Autre moyen de contact

Sans objet

2.7. Adresse électronique

Si vous devez contacter le CSIRT CNES, veuillez nous contacter à : csirt-cnes@cnes.fr

2.8. Clé publique et information sur le chiffrement

Le CSIRT CNES utilise la clé de chiffrement suivante :

- Identifiant : 0220CD9D81D17096
- Empreinte : a21dd67ad8f313b904430bff0220cd9d81d17096

La clef publique est disponible à l'adresse http://pgp.mit.edu/ ou sur simple demande auprès du CSIRT CNES.

2.9. Membres de l'équipe

L'équipe du CSIRT CNES est constituée d'experts en sécurité des systèmes d'information : expert en traitement d'incidents, analyse des vulnérabilités, forensique, etc.

2.10. Autres informations

La confidentialité des informations échangées avec le CSIRT CNES repose sur l'utilisation du protocole TLP (Traffic Light Protocol). Ce protocole définit la confidentialité attendue par l'émetteur quant aux informations échangées, à l'aide d'un marquage spécifique apposé par ce dernier.

En l'absence d'un marquage TLP explicite, toute donnée échangée sous quelques formes que ce soit est considérée marquée TLP AMBER.

Au sein du CNES, il sera fait application de la directive du CNES quant à la protection des informations.

2.11. Point de contact pour les bénéficiaires des services

Pour tout contact avec le CSIRT CNES, le canal de communication à privilégier est l'adresse mail indiquée ci -avant.

En cas d'urgence, veuillez spécifier la balise [URGENT] dans le champ objet de votre email.

3. Charte

3.1. Ordre de mission

L'objectif du CSIRT CNES est triple :

-d'une part traiter tous les incidents ayant trait à l'espionnage et à la fuite de données, consécutif à un ransomware, concernant les systèmes d'information régulés du CNES. Dans chacun de ces cas, les équipes du CSIRT organisent et coordonnent la réponse à incident.
-d'autre part, de traiter les demandes de renseignement (forensique, signaux faibles, sabotage, etc.),
-Enfin avoir un rôle de prévention en prévenant les cyberattaques, en améliorant la prise de conscience et la résilience en cyber sécurité.

Au sein de l'InterCERT France, le CSIRT CNES contribuera aux échanges pour tous les acteurs de la communauté spatiale.

Le pilotage du CSIRT CNES est assuré au sein de la Direction Centrale de la Sûreté et de la Sécurité Industrielle (cf. $3.4).

Les missions du CSIRT CNES couvrent la réponse à incidents ainsi que la prévention :

- La gestion les incidents cyber identifiés ci-avant ;
- Le pilotage d'une réunion hebdomadaire avec les responsables du SOC et les responsables cyber du CNES ;
- La tenue à jour de fiches réflexes pour le traitement des incidents ;
- La tenue d'une cartographie des systèmes d'informations ;
- L'identification et la tenue à jour de la liste des RSSIs pour l'ensemble des systèmes informatiques du CNES ainsi que la mise en œuvre /tenue d'un annuaire des correspondants du secteur ;
- L'assistance à la prévention des incidents de sécurité avec notamment la diffusion de mesures de protection nécessaires ;
- L'organisation du partage d'informations quant aux incidents avec les partenaires et industriels du secteur ;
- Le partage des informations sur les vulnérabilités cyber, les menaces et les attaques et en diffusant les alertes et avertissements provenant de différentes sources ;
- La prise en charge de la gestion de crise cyber au sein du CNES.

Dans un premier temps et par facilité, le périmètre visé sera celui des systèmes CNES faisant l'objet d'une supervision par le SOC ; une extension du périmètre sera réalisée progressivement (systèmes régulés, systèmes métiers (orbitaux, lanceurs), systèmes non supervisés par le SOC).

3.2. Entités bénéficiant du service

Le CSIRT CNES est une structure interne au CNES adossée au SOC.

Le périmètre d'intervention du CSIRT CNES couvre l'ensemble des centres du CNES : Centre Spatial de Toulouse, Centre Spatial de Guyane, Siège et Paris Daumesnil (Direction du Transport Spatial). Plus opérationnellement, ses services sont disponibles pour tous les projets pilotés par le CNES, pour tous les RSSIs de systèmes informatiques, pour l'ensemble de la communauté cyber du CNES.

3.3. Support et/ou relations

Le CSIRT CNES dispose d'un canal d'échange privilégié avec les CSIRTs des industriels du secteur, l'InterCERT France, les CSIRTs régionaux, les CSIRTs industriels.

3.4. Autorité

La Direction de la Sûreté et de la Sécurité Industrielle assure la maîtrise d'ouvrage (services, roadmap de l'offre de service, cohérence avec les activités dédiées à la détection) et le pilotage opérationnel des activités du CSIRT du CNES.

CSIRT CNES RFC 2350

4. Politiques

4.1. Types d'incidents et niveau d'intervention

Le SOC enregistre et qualifie tous les incidents de sécurité.

Le CSIRT CNES gère tous les incidents ayant trait à l'espionnage et à la fuite de données, les incidents consécutifs à un ransomware et tous les incidents concernant les systèmes d'information régulés. Dans ces trois cas, les équipes du CSIRT organisent et coordonnent la réponse à incident. Les missions du CSIRT CNES sont décrites au $3.1.

Les opérations du CSIRT CNES sont conformes à la législation française. Si besoin, le CSIRT CNES peut être impliqué par les autorités françaises sur tout incident.

Le CSIRT CNES peut aussi bénéficier d'un appui technique du CERT-FR mais ne se substitue pas à ce dernier.

4.2. Coopération, interaction et divulgation d'informations

Toutes les communications externes du CSIRT CNES respectent le protocole TLP.

Les informations relatives à un incident telles que le nom de la structure et les détails techniques ne sont pas publiées à l'extérieur du CNES sans l'accord de l'OCSSI ou son représentant.

Le CSIRT CNES peut publier un retour d'expérience présentant l'incident et la réponse apportée (technique d'attaque, mesures de confinement, mesures de remédiation) à des fins de prévention et de réaction à cette spécificité d'incidents.

Le CSIRT CNES peut être amené à communiquer des informations au CERT-FR lorsque ce dernier sollicite son appui.

Pour accomplir ses missions, le CSIRT CNES peut être amené à échanger des informations avec d'autres CSIRTs, fournisseurs, etc.

4.3. Communication et authentification

Le moyen de communication privilégié est la messagerie électronique. Les informations sensibles sont chiffrées avant d'être transmises. En fonction des acteurs, le CSIRT CNES utilise Zed ! pour garantir la confidentialité et l'intégrité des documents échangés en interne.

CSIRT CNES RFC 2350

5. Services

5.1. Activités proactives

5.1.1.Promotion des mesures de protection nécessaires

Le CSIRT CNES fournit à ses correspondants un guide des bonnes pratiques en matière de cybersécurité.

5.1.2. Partage d'informations

Le CSIRT CNES fournit à ses correspondants une veille sur l'actualité de la sécurité des SI et sur les menaces propres au secteur du spatial. Elle informe et alerte les acteurs au travers de la publication de bulletins de sécurité portant :

- Sur les technologies standards (émergence de menaces, méthodologies d'attaques innovantes, nouvelles vulnérabilités) et spécifiques au secteur spatial (incidents de sécurité, nouvelles vulnérabilités) ;
- Sur des alertes de sécurité et de recommandations pour se protéger des menaces en cours ;
- Sur des documents d'appui à la gestion de la sécurité et des incidents (fiches réflexes, fiches pratiques, guides de bonnes pratiques).

Pour réaliser cette activité, le CSIRT dispose d'une capacité de threat intelligence et d'outils spécifiques permettant le suivi de la gestion des vulnérabilités :

- Maintien d'une liste des sources de veille en matière de menaces, de vulnérabilités et de correctifs ;
- Capitalisation et paramétrage d'un outil de détection ;
- Formalisation d'un processus permettant de cadrer l'activité (rédaction des premières procédures de correctifs, templates de rapport de vulnérabilités) ;
- Assurer une première activité de gestion des vulnérabilités ;
- Déploiement d'une plateforme permettant de centraliser l'activité (scan et suivi des correctifs).

5.2. Activités réactives

5.2.1. Réponse aux incidents

Le service de réponse aux incidents est disponible de 9h à 18h les jours ouvrés.

L'enregistrement, la qualification et le traitement des incidents est de la responsabilité du SOC sauf les types d'incidents identifiés dans le $4.1 pour lesquels le CSIRT prend en charge la réponse à incident. Dans ce contexte, l'accompagnement et l'appui mis en place par le CSIRT CNES consistent à :

- Récupérer le signalement des évènements indésirables et notifier au déclarant sa prise en compte par le CSIRT CNES ;
- Qualifier l'incident ;
- Apporter un support au traitement des incidents aux acteurs cybersécurité identifiés, formuler des recommandations et notamment proposer des mesures d'urgence pour limiter l'impact

de celui-ci, des mesures de remédiation ainsi que des mesures destinées à améliorer la sécurité du ou des systèmes d'information concernés.

5.2.2. Coordination

Les actions réalisées peuvent être les suivantes :

- Accompagner la structure concernée dans le traitement de l'incident de sécurité des systèmes d'information ;
- Organiser, planifier des exercices de crises cyber ;
- Le cas échéant, préparer une alerte vers les autorités compétentes de l'Etat selon la nature de l'incident.

5.2.3. Résolution

Les actions réalisées sont les suivantes :

- Selon le niveau de maturité, du conseil sur les mesures appropriées à mettre en place/ œuvre pour faire progresser le niveau de protection,
- Le cas échéant, rédiger un retour d'expérience sur la gestion de l'incident.
- Suivre le processus de résolution des incidents.

6. FORMULAIRE DE NOTIFICATION D'INCIDENTS

La déclaration des incidents de sécurité des systèmes d'information pour les membres s'effectue par mail à l'adresse indiquée ci-avant.

7. DECHARGE DE RESPONSABILITE

Bien que toutes les précautions aient été prises dans l'élaboration des bulletins de sécurité, le CSIRT CNES ne peut être tenu responsable des erreurs ou omissions, ou des dommages pouvant résulter de l'utilisation des informations brutes fournies dans le cadre de l'appui au traitement d'un incident ou publiées ou issues de ses publications.