Titre du document :

CERT-CEA – RFC 2350

Description du CERT-CEA conformément aux spécifications de la RFC 2350.

Historique des évolutions d'indice :

Indice	Date	Nature des modifications
1	22/11/2023	Création du document

Direction de la sécurité et de la sûreté nucléaire / Service de sécurité des systèmes d'information
Commissariat à l'énergie atomique et aux énergies alternatives
Centre de Paris-Saclay – Établissement de Fontenay-aux-Roses – B.P. 6 – 92265 Fontenay-aux-Roses Cedex
✉ cert@cea.fr

SOMMAIRE

1. CONCERNANT CE DOCUMENT

1.1 Version

La version de ce document est la 1, publiée le 22/11/2023.

1.2 Notification des changements

Les modifications apportées à ce document ne sont pas notifiées.

1.3 Lieu de publication

La dernière version du document est disponible à l'adresse : https://www.cea.fr/cert/

1.4 Authenticité

Ce document est signé par la clé PGP du CERT-CEA.

La signature est disponible à l'adresse : https://www.cea.fr/cert/rfc2350.sig

1.5 Identification

Titre : CERT-CEA – RFC 2350

Version : 1

Date du document : 22/11/2023

Expiration : ce document est valide jusqu'à ce qu'il soit remplacé par une version ultérieure

2. CONTACTS

2.1 Nom

Nom court : CERT-CEA

Nom officiel : Service de sécurité des systèmes d'information de la Direction de la sécurité et de la sûreté nucléaire

2.2 Adresse

CERT-CEA

DSSN/S3I - bat 19

18 route du Panorama, B. P. 6

92265 Fontenay-aux-Roses cedex

France

2.3 Fuseau horaire

CET/CEST : Paris (UTC+01:00, et UTC+02:00 heure d'été)

2.4 Numéro de téléphone

+33 6 85 82 64 32

2.5 Numéro de FAX

Non disponible.

2.6 Autre canal de communication

Non disponible.

2.7 Adresse de courrier électronique

L'adresse de courrier électronique du CERT-CEA est : cert@cea.fr

2.8 Clé publique et informations de chiffrement

Le CERT-CEA possède une clé publique PGP :

- ID utilisateur: CERT-CEA <cert@cea.fr>
- ID clé: 0xD1DF1C6C
- Empreinte digitale: 30BC9DD6816F3804C10DC82B4BEDCC8BD1DF1C6C

La clé publique du CERT-CEA est disponible sur le site https://www.cea.fr/cert/ ou peut être obtenue en envoyant une demande à cert@cea.fr ou depuis les serveurs de clés habituels.

2.9 Composition de l'équipe

L'équipe est constituée d'ingénieur.es en cybersécurité.

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

2.10 Horaires de fonctionnement

Les heures ouvrées concernant le CERT-CEA sont du lundi au vendredi de 08h30 à 17h10.

2.11 Points de contact

Le CERT-CEA est contacté de préférence par mail à l'adresse cert@cea.fr. À défaut il est possible de le contacter par téléphone en journée.

3. CHARTE

3.1 Missions

La Direction de la sécurité et de la sureté nucléaire (DSSN) a pour mission de garantir que le CEA remplit ses obligations en matière de « sécurité et sûreté nucléaire ». À cet effet, la DSSN propose la politique de sécurité du CEA et l'organisation correspondante, traduit cette politique en instructions et recommandations et veille à leur mise en œuvre. La DSSN est l'interlocuteur désigné des autorités publiques nationales compétentes dans ce domaine.

Au sein de la DSSN, le Service de sécurité des systèmes d'information (S³I) est en charge de la coordination des activités de lutte informatique défensive (cyberdéfense) pour les activités du CEA.

Le CERT-CEA est l'entité de DSSN/S³I chargée des missions suivantes :

- conception et exploitation de l'infrastructure de supervision (SOC) couvrant l'ensemble des réseaux interconnectés du CEA, pour la détection, l'analyse et le déclenchement des incidents de sécurité ;
- coordination de la réponse aux incidents de cybersécurité et suivi de leur résolution ;
- réalisation des investigations numériques pour déterminer l'origine des attaques, leur méthodologie, et adapter la supervision en conséquence ;
- gestion de la menace par la veille en sources ouvertes et les échanges avec d'autres entités ;
- tests intrusifs sur les systèmes internes pour en éprouver la sécurité, s'assurer de l'efficacité de la supervision, et proposer des améliorations.

3.2 Périmètre d'action

Le CERT-CEA intervient sur l'ensemble des composants des systèmes d'information du périmètre de l'AQSSI CEA : utilisateurs et utilisatrices, systèmes, applications et réseaux.

3.3 Parrainage et affiliation

Le CERT-CEA est un CSIRT privé. Il maintient des relations avec les différents CERT et CSIRT nationaux et internationaux ; ainsi qu'avec les CERT internes du CEA spécifiques à chaque site.

3.4 Autorité

Le CERT-CEA est placé sous l'autorité du Directeur de la sécurité et de la sureté nucléaire du Commissariat à l'énergie atomique et aux énergies alternatives, également Autorité qualifiée de la sécurité des systèmes d'information.

4. POLITIQUES

4.1 Types d'incidents et niveau de support

Le CERT-CEA assure un premier diagnostic et coordonne tout incident de sécurité informatique qui cible ou pourrait cibler son périmètre d'action. En fonction de la nature de l'incident, le CERT-CEA informe les acteurs en capacité d'y remédier. La résolution de l'incident est suivie pour s'assurer de son efficacité, établir des statistiques, capitaliser, et améliorer les capacités de diagnostic.

Le niveau de service offert par le CERT-CEA varie en fonction du type d'incident, de sa criticité, et des ressources disponibles pour le prendre en charge.

4.2 Coopération, échanges, et confidentialité de l'information

Le CERT-CEA échange les informations nécessaires avec les autres CERT/CSIRT susceptibles d'être concernés selon le besoin d'en connaître. Le partage d'information se fait dans le respect des différentes règlementations de protection existantes et respectera le CSIRT Code of Practice (https://www.trusted-introducer.org/TI-CCoP.pdf).

Les renseignements généraux relatifs aux incidents sont échangés avec les parties concernées dans le périmètre d'action ainsi qu'avec les groupes de coopération CERT/CSIRT. Les informations nominatives ne sont pas transmises à des tiers à moins que la loi ne l'exige.

Le CERT-CEA traite l'information dans des environnements physiques et techniques sécurisés conformément aux réglementations existantes en matière de protection de l'information.

4.3 Communication

Le CERT-CEA applique le protocole de partage d'informations (TLP) comme décrit à l'adresse : https://www.cert.ssi.gouv.fr/csirt/politique-partage/

L'échange d'information sensible par courrier électronique se fait de façon chiffrée avec PGP. Les mêmes règles s'appliquent aux transferts de fichiers.

5. SERVICES

5.1 Réponse à l'incident

Le CERT-CEA propose les services suivants dans le cadre de la réponse à l'incident de sécurité informatique :

- détection des incidents ou réception de leur signalement ;
- diagnostic, analyse technique, corrélation et triage des incidents ;
- signalement des incidents aux équipes en capacité d'intervenir ;
- assistance à résolution et contrôle des remédiations ;
- coordination avec les autres entités hors du périmètre d'action.

5.2 Alertes et Cyberthreat Intelligence

Afin d'adapter ses capacités de diagnostic, le CERT-CEA réalise une veille sur les menaces, les vulnérabilités, les scénarios d'attaques et les mesures de sécurité nécessaires.

Le CERT-CEA assure aussi une sensibilisation et une communication à destination de son périmètre d'action destinées à prévenir les risques et limiter leurs conséquences.

6. FORMULAIRE DE DÉCLARATION D'INCIDENT

Aucun formalisme n'est demandé pour le signalement ou la déclaration d'incident. Ils sont adressés par courrier électronique à l'adresse cert@cea.fr en précisant autant que possible les systèmes concernés et les horaires des événements.

7. DÉCHARGE DE RESPONSABILITÉ

Bien que toutes les précautions d'usage et vérifications aient été prises lors de la communication de toute information, le CERT-CEA se décharge de toute responsabilité pour les erreurs, omissions, et préjudices résultant des informations fournies.

Si vous constatez une erreur dans ce document merci de nous le signaler par mail et nous tâcherons de rectifier les informations au plus vite.