CERT-Hexanet

RFC2350

SOMMAIRE

1. Informations sur le document

Ce document contient une description du CERT-HEXANET conformément à la spécification RFC 2350. Il fournit des informations de base sur le CERT-HEXANET, décrit ses responsabilités, les services offerts et les moyens de le contacter.

1.1 DATE DE LA DERNIERE MISE A JOUR

Version 1.0, publiée le 26 mars 2025

1.2 LISTE DE DISTRIBUTION DES NOTIFICATIONS

Il n'y a pas de liste de distribution pour les notifications

1.3 OÙ TROUVER CE DOCUMENT

La version actuelle et la plus récente de ce document est disponible à l'adresse suivante :

https://cybersecurite.hexanet.fr/cert-gestion-des-incidents-de-securite-informatique/CERT-Hexanet_RFC2350_FR.pdf

1.4 AUTHENTICITÉ DU DOCUMENT

Ce document a été signé cryptographiquement avec la clé privée PGP du CERT-Hexanet.

La signature, la clé publique PGP, son identifiant et son empreinte sont disponibles sur le site Internet du CERT-Hexanet à l'adresse suivante :

https://cybersecurite.hexanet.fr/cert-gestion-des-incidents-de-securite-informatique

1.5 IDENTIFICATION DU DOCUMENT

Titre du document : CERT-HEXANET_RFC2350_FR

Version : 1.0

Date de création du document : 10 octobre 2024

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

2. Informations de contact

2.1 NOM DE L'ÉQUIPE

Nom court : CERT-Hexanet

Nom Long : Centre de réponse aux incidents de sécurité interne et commercial d'Hexanet

2.2 ADRESSE

Hexanet

3 All. Albert Caquot

51100 Reims, France

2.3 FUSEAU HORAIRE

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

2.4 NUMÉRO DE TÉLÉPHONE

+33 (0)3 26 85 85 60

2.5 NUMÉRO DE FAX

Non disponible

2.6 AUTRES MOYENS DE COMMUNICATIONS

Non disponible

2.7 ADRESSE DE COURRIER ÉLECTRONIQUE

Afin de nous notifier d'un incident de sécurité ou d'une menace informatique ciblant ou impliquant votre organisation ou le CERT-Hexanet, contactez-nous à cert@hexanet.fr.

Cette adresse de courrier électronique est surveillée par les membres du CERT pendant les jours ouvrées du lundi au vendredi de 08h30 à 18h00 CET/CEST.

Nous opérons en dehors de ces jours et heures uniquement en cas d'urgence.

2.8 CLE PUBLIQUE ET INFORMATIONS LIEES AU CHIFFREMENT

PGP est utilisé afin de garantir la confidentialité et l'intégrité des échanges (notifications, signalement d'incident, etc.) avec le CERT-Hexanet

Identifiant de l'utilisateur : CERT-Hexanet (Centre de reponse aux incidents de securite interne et commercial Hexanet) <cert@hexanet.fr>

Identifiant court de la clé : 0x5B4AE7A5

Identifiant long de la clé : 0xCA18F8D25B4AE7A5

Empreinte numérique : D6FF 6779 527F 2B4A DFF6 14B2 CA18 F8D2 5B4A E7A5

La clé publique est disponible en utilisant le lien suivant :

https://cybersecurite.hexanet.fr/cert-gestion-des-incidents-de-securite-informatique

Elle peut aussi être récupérée depuis les serveurs de clé publique suivants :

- https://pgp.circl.lu/
- https:// keys.openpgp.org /

2.9 MEMBRES DE L'ÉQUIPE

Le responsable de l'équipe du CERT-Hexanet est Pascal Abraham

L'équipe du CERT-Hexanet est composé d'analystes sécurité d'Hexanet Cybersécurité

2.10 AUTRES INFORMATIONS

Les informations générales concernant le CERT-Hexanet sont accessibles en utilisant l'URL suivante :

https://cybersecurite.hexanet.fr/cert-gestion-des-incidents-de-securite-informatique

2.11 POINTS DE CONTACT AVEC LES CLIENTS

La méthode à privilégier pour contacter le CERT-Hexanet est l'envoie d'un courrier électronique à l'adresse cert@hexanet.fr.

Cette adresse de courrier électronique est surveillée par les membres du CERT-Hexanet pendant les jours ouvrées du lundi au vendredi de 08h30 à 18h00 CET/CEST.

Le CERT opère en dehors des jours et heures ouvrés seulement en cas d'urgence.

En cas d'urgence en heures non ouvrés, contactez le CERT-Hexanet par téléphone au +33 (0)3 26 85 85 60

3. Charte

3.1 ORDRE DE MISSION

Le CERT-Hexanet est un CERT privé fournissant des services de sécurité en France et en Europe.

Le CERT-Hexanet a aussi la charge de la gestion des incidents de sécurité impactant Hexanet.

Son objectif est double :

- Assister dans l'implémentation de mesures proactives afin de réduire les risques d'incidents de sécurité
- Assister dans la réponse aux incidents de sécurité dans les cas où ils surviendraient

Le CERT-Hexanet opère en accord avec les valeurs clés suivantes :

- Le CERT-Hexanet s'efforce d'opérer selon les plus hauts standards d'éthique, d'intégrité, d'honnêteté et de professionnalisme
- Le CERT-Hexanet est dévoué à la délivrance de services de grande qualité à ses bénéficiaires
- Le CERT-Hexanet s'assure de répondre aux incidents de sécurité de la manière la plus efficace possible
- Le CERT-Hexanet s'assure de faciliter les échanges de bonnes pratiques parmi ses bénéficiaires et avec ses pairs

3.2 BÉNÉFICIAIRES

Le principal bénéficiaire du CERT-Hexanet est le système d'information d'Hexanet composé de ses utilisateurs, systèmes, applications et réseaux.

Malgré ce qui précède, étant un CERT commercial, le CERT-Hexanet délivre aussi des services à sa communauté de client ayant souscrit un contrat de support.

3.3 AFFILIATION

Le CERT-Hexanet fait partie d'Hexanet : https://www.hexanet.fr/

Le CERT-Hexanet maintien des relations avec les équipes des différents CSIRT et CERT nationaux et internationaux.

3.4 AUTORITÉ

Pour les besoins interne, le CERT-Hexanet opère sous l'autorité du directeur général d'Hexanet.

Pour les incidents externes, le CERT-Hexanet coordonne les incidents de sécurité pour le compte de ses bénéficiaires et uniquement sur demande de ces derniers.

4. Politiques

4.1 TYPES D'INCIDENTS ET NIVEAU D'INTERVENTION

Le CERT-Hexanet adresse tout type d'incident de sécurité pouvant impacter Hexanet ou la communauté de client du CERT-Hexanet.

Le niveau de support apporté par le CERT-Hexanet varie en fonction du type et de la sévérité de l'incident, des potentiels impacts, du type du bénéficiaire, de la taille de la communauté d'utilisateurs affectés et des ressources du CERT-Hexanet à ce moment-là. En fonction du type d'incident, le CERT-Hexanet déploiera progressivement ses services incluant mais non limités à la réponse aux incidents et l'investigation numérique.

Le CERT-Hexanet, travaille en collaboration avec les équipes internes d'Hexanet et peut se reposer sur leurs compétences.

4.2 COOPÉRATION, INTERACTION ET PARTAGE D'INFORMATION

Le CERT-Hexanet reconnait l'importance primordiale de la coordination opérationnelle et du partage d'informations entre les CERT, CSIRT, SOC, ainsi qu'avec d'autres organisations, qui pourraient l'aider à fournir ses services ou apporter des avantages à ses bénéficiaires.

Par conséquent, le CERT-Hexanet peut être amené à échanger des informations avec d'autres organisations qui pourraient lui apporter une aide pour délivrer ses services, en particulier pour la résolution des incidents. Cependant, aucune donnée personnelle ou générale n'est échangée sauf autorisation explicite. De plus, en cas d'échange

d'informations, le CERT-Hexanet protège la confidentialité des informations liées à ses bénéficiaires en les anonymisant.

Toutes les informations échangées avec un bénéficiaire durant un incident (Données personnelles, configurations système, vulnérabilités connues et leurs emplacements) sont stockées dans un environnement sécurisé et chiffrées si nécessaire.

Le CERT-Hexanet traite les informations en accord avec le protocole Traffic Light Protocol (TLP) version 1.1 et 2. Elle respecte la politique de partage d'informations défini par le FIRST à https://www.first.org/tlp, lorsqu'il reçoit des informations marquées en utilisant le protocole TLP.

Les informations opérationnelles provenant du CERT-Hexanet, sont également marquées TLP, et sont à prendre en compte par les destinataires.

Le CERT-Hexanet opère sous les restrictions imposées par les lois françaises.

4.3 COMMUNICATION ET AUTHENTIFICATION

Le CERT-Hexanet protèges les informations sensibles conformément aux réglementations et politiques en vigueur en France et dans l'UE.

Le CERT-Hexanet respecte les marquages de sensibilité attribués par les émetteurs d'informations communiqués au CERT-Hexanet.

L'échange d'informations non sensibles, devrait être réalisé en utilisant le courrier électronique non chiffré.

L'échange d'informations sensibles et la communication authentifiée est réalisée par le CERT-Hexanet en utilisant PGP pour chiffrer et/ou signer les messages.

Toute communication sensible au CERT-Hexanet doit être chiffrée avec notre clé publique PGP (Défini en section 2.8)

5. Services

5.1 RÉPONSE AUX INCIDENTS

Le CERT-Hexanet effectue de la réponse aux incidents pour ses bénéficiaires (Définis en section 3.2)

Le CERT-Hexanet prend en charge les aspects de triage et de coordination des incidents impliquant le périmètre de ses bénéficiaires. La résolution technique des

incidents est de la responsabilité du bénéficiaire. Cependant, le CERT-Hexanet proposera un accompagnement et des conseils sur demande du bénéficiaire.

Sans exhaustivité, les aspects suivants sont couverts par le CERT-Hexanet :

5.1.1 TRIAGE

- Prise en compte du signalement et prise de contact avec le déclarant
- Confirmation ou non de l'incident
- Evaluation du périmètre et de l'impact de l'incident

5.1.2 COORDINATION

- Déterminaison du vecteur d'attaque initial
- Réalisation de la collecte et de l'analyse des données de preuves numériques (Analyse des journaux système/réseau, mémoire volatile et non volatile, etc.)
- Facilitation du contact avec d'autres sites susceptibles d'être impliqués
- Facilitation du contact avec les forces de l'ordre compétentes si nécessaire et si demandé par le bénéficiaire
- Echange d'informations avec d'autres CSIRT/SOC/CERT si accord du bénéficiaire

5.1.3 RESOLUTION

- Fourniture d'un plan d'action et d'une assistance aux équipes techniques du bénéficiaire afin de remédier au vecteur d'attaque initial
- Fourniture d'un plan d'action et d'une assistance aux équipes techniques du bénéficiaire afin de sécuriser le système d'information compromis
- Evaluation de la vraisemblance des actions à fournir des résultats proportionnellement à leurs coûts et risque. Notamment pour les actions visant une éventuelle poursuite ou sanction disciplinaire : collecte de preuves a posteriori, observation des actions d'un attaquant, mise en place de pièges pour les attaquants, etc.
- Fourniture d'un plan d'action et d'une assistance pour la collecte de preuves lorsque des poursuites pénales ou des mesures disciplinaires sont envisagées

5.2 ACTIVITÉS PROACTIVES

Le CERT-Hexanet réalise et fournit les activités proactives suivantes à ses bénéficiaires :

- Veille technologique
- Partage d'informations sur les menaces et vulnérabilités majeures
- Partage d'informations sur les nouveaux outils et techniques d'attaque
- Partage d'informations sur les mesures et recommandations de sécurité

6. Formulaires de notification d'incident

Aucun formulaire de déclaration d'incident n'est fourni et n'est nécessaire pour déclarer un incident au CERT-Hexanet. Dans la mesure du possible, les incidents doivent être signalés par courrier électronique à cert@hexanet.fr, de préférence chiffré avec notre clé publique PGP (Défini en section 2.8)

Si possible, une déclaration d'incident doit contenir les informations suivantes :

- Les informations de contact, incluant une adresse de courrier électronique et un numéro de téléphone
- La date et l'heure du début de l'incident
- La date et l'heure de la détection de l'incident
- Une brève description de l'incident
- L'impact estimée de l'incident
- La liste et la description des actifs impactés (Adresse IP, FQDN, URL)
- La liste des mesures prise Jusqu'alors
- Toute autre information telle que les détails des observations ayant menées à la découverte de l'incident (extraits de journaux, tout autre information technique)

Dans le cas où, vous voudriez nous transférer un courrier électronique suspect/malveillant dans le cadre de la déclaration d'un incident, assurez-vous que les toutes les entêtes, le corps et les pièces jointes soient inclus.

7. Décharges de responsabilité

Bien que toutes les précautions soient prises dans la préparation des informations, notifications et alertes, CERT-Hexanet n'assume aucune responsabilité pour les erreurs ou omissions, ou pour les dommages résultant de l'utilisation, des informations contenues.