CERT-Asinhpa
RFC 2350

Table des matières

1 A propos de ce document

Ce document contient une description du CERT-Asinhpa conformément à la RFC 23501.

Il fournit des informations essentielles sur le CERT-Asinhpa, détaillant ses responsabilités et les services fournis.

1.1 Date de dernière mise à jour

- V1.0 : 11/2023 - Novembre 2023
- V1.1 : 04/2024 - Avril 2024
- V1.2 : 09/2024 - Septembre 2024

1.2 Liste de diffusion des notifications

Aucune liste de diffusion n'est disponible pour les mises à jour de ce document.

1.3 Lieu de distribution de ce document

La version actuelle la plus récente de ce document est disponible sur le site web du CERT-Asinhpa à l'adresse : https://asinhpa.org/cert-asinhpa

1.4 Authenticité de ce document

Ce document a été signé avec la clé PGP du CERT-Asinhpa.
La signature et notre clé PGP publique (ID et empreinte) sont disponibles sur notre site web au lien suivant : https://asinhpa.org/ressources-et-realisations-asinhpa

1.5 Identification du document

Titre : "CERT-Asinhpa_RFC2350_FR"
Version : 1.2
Date du document : Septembre 2024
Expiration : Ce document est valide jusqu'à ce qu'il soit remplacé par une version ultérieure.

2 Informations sur le CERT-Asinhpa

2.1 Nom de l'entité

Nom complet : CERT-Asinhpa

2.2 Adresse

Alliance du numérique éthique et souverain en santé

CERT-Asinhpa
4 Rue du Professeur Jean Pecker, CS 76513 35065 Rennes Cedex
France

2.3 Zone de temps

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

2.4 Numéro de téléphone

Sans objet.

2.5 Numéro de fax

Sans objet.

2.6 Autre moyen de contact

Sans objet.

2.7 Adresse électronique

Si vous avez besoin de signaler au CERT-Asinhpa un incident de cybersécurité ou un acte de cyber malveillance lié aux membres de l'Asinhpa, vous pouvez le joindre à l'adresse suivante : cert@asinhpa.org

2.8 Clé publique et information sur le chiffrement

PGP est utilisé pour les échanges fonctionnels avec le CERT-Asinhpa.

- Empreinte digitale pub rsa4096/0x9053966DDC788625 2024-10-14 [SCE] [expire : 2034-10-12]
- Empreinte de la clef = E130 A3B6 EF56 DC8B 6C94 8D0E 9053 966D DC78 8625
  uid CERT ASINHPA (CERT Key ID) cert@asinhpa.org

La clé PGP publique est disponible à l'emplacement suivant : https://asinhpa.org/ressources-et-realisations-asinhpa

2.9 Membres de l'équipe

L'équipe du CERT-Asinhpa est constituée d'experts en sécurité informatique mis à disposition par les membres de l'Asinhpa.

Le CERT-Asinhpa ne comprend à ce jour aucune ressource en propre, à l'exception de la chargée de mission de l'Asinhpa.

La liste des membres de l'équipe du CERT-Asinhpa n'est pas publiquement disponible.

L'identité des membres de l'équipe du CERT-Asinhpa pourrait être divulguée au cas par cas en fonction du besoin d'en connaître.

2.10 Autres informations

Consultez notre site web à l'adresse https://asinhpa.org/ pour obtenir des informations supplémentaires sur le CERT-Asinhpa et sur les membres de l'Asinhpa.

2.11 Point de contact pour les acteurs de santé

Le CERT-Asinhpa préfère recevoir les rapports d'incidents par e-mail à l'adresse .

Vous pouvez utiliser notre clé cryptographique pour assurer l'intégrité et la confidentialité. En cas d'urgence, veuillez utiliser l'étiquette [URGENT] dans le champ « sujet » de votre e-mail.

Les heures d'opération du CERT-Asinhpa sont du lundi au vendredi de 9h à 17h.

3 Charte

3.1 Ordre de mission

Le CERT-Asinhpa est le Computer Emergency Response Team (CERT) interne de l'Asinhpa. Sa mission consiste à faciliter le partage d'information sur les menaces et les incidents pouvant affecter les membres de l'Asinhpa ou leurs clients.

Les membres du CERT-Asinhpa sont également en mesure de coordonner et enquêter sur les réponses aux incidents de sécurité informatique affectant un ou plusieurs des adhérents.

Le CERT-Asinhpa agit uniquement pour le compte et en direction des adhérents de l'Asinhpa. Il est en relation avec le CERT-FR et le CERT Santé et peut-être amené à communiquer avec les clients ou partenaires des adhérents de l'Asinhpa.

Les missions du CERT-Asinhpa sont :

- Aider à prévenir les incidents de sécurité en mettant en place les mesures de protection nécessaires et en partageant des bonnes pratiques
- Partager des informations sur les menaces avec les membres de l'Asinhpa
- Soutenir la réponse aux incidents des membres de l'ASINHPA avec le soutien de partenaires de confiance si nécessaire.

3.2 Entités bénéficiant du service

Peuvent bénéficier du service du CERT-Asinhpa, les organismes qui satisfont l'ensemble des conditions suivantes :

- Membres de l'Asinhpa ayant une activité d'hébergeur de données de santé;
- Participants au GT SSI de l'Asinhpa ;
- Qui ont signé la charte constitutive du CERT-Asinhpa.

3.3 Support et/ou relations

Seuls les membres de l'Asinhpa qui ont signé la charte constitutive du CERT-Asinhpa peuvent mettre à disposition des ressources au sein de l'équipe du CERT tel que défini en 2.9.

Les autres membres de l'Asinhpa pourront recevoir des notifications du CERT-Asinhpa mais n'auront pas accès aux documents réservés à l'équipe CERT-Asinhpa et ne pourront pas avoir accès aux outils CERT (email, instance MISP interne…).

3.4 Autorité

Le CERT-Asinhpa mène ses activités sous la supervision des membres de l'Asinhpa.

4 Politiques

4.1 Types d'incidents et niveau d'intervention

Le CERT-Asinhpa est le point central de contact en ce qui concerne les incidents informatiques liés à la sécurité des organismes membres de l'Asinhpa.

Les services du CERT-Asinhpa comprennent des services réactifs et proactifs :

- Service de permanence du lundi ou vendredi de 9h à 17h.
- Information de sécurité et alertes.
- Assistance et soutien à la réponse aux incidents entre les membres du Cert-Asinhpa.

Le CERT-Asinhpa peut aussi bénéficier d'un appui technique du CERT Santé.

4.2 Coopération, interaction et divulgation d'informations

Les informations relatives à un incident telles que le nom de la structure et les détails techniques ne sont pas publiées sans l'accord des parties prenantes impliquées membres de l'Asinhpa. Sauf indication contraire, les informations fournies sont traitées de manière confidentielle et dans le respect du TLP.

Le CERT-Asinhpa peut être amené à communiquer des informations au CERT-FR ou/et au CERT

Santé et/ou à un PRIS lorsqu'elle sollicite son appui ou lorsque cela concerne un bénéficiaire du CERT Santé.

Les informations seront transmises en fonction de son marquage TLP et du principe du « besoin d'en connaitre ».

Le CERT-Asinhpa ne transmettra jamais d'informations confidentielles à des tiers non-cités ci-dessus sauf si cela est exigé par la loi ou en cas d'accord explicite de l'ensemble des parties concernées.

4.3 Communication et authentification

La méthode de communication privilégiée est l'e-mail. Pour l'échange d'informations sensibles et la communication authentifiée, CERT-Asinhpa utilise PGP pour chiffrer et/ou signer les messages. Toute communication sensible adressée à CERT-Asinhpa doit être chiffrée avec notre clé PGP publique, comme indiqué dans la Section 2.8.

5 Services

5.1 Activités réactives

5.1.1 Réponse aux incidents

Les services de réponse aux incidents du CERT-Asinhpa sont disponibles en heures ouvrées pour les organismes membres. Tous les incidents liés aux technologies de l'information et de la communication reçus par le CERT-Asinhpa sont évalués et transmis aux membres de l'Asinhpa concernés.

5.1.2 Triage

Les organismes membres de l'Asinhpa prennent en charge :

- Évaluation de la gravité de l'incident (premier niveau de réponse)
- Information du (des) membre(s) concerné(s) et dissémination de l'information au sein du CERT-Asinhpa en fonction du TLP et du besoin d'en connaitre
- Si nécessaire, escalade vers les autorités compétentes de l'Etat selon la nature de l'incident :
    - A l'ANSSI en cas d'incident majeur de cybersécurité pouvant impacter d'autres secteurs.
    - Au CERT Santé dans le cas d'un incident majeur dans un établissement de santé
    - A la Commission Nationale de l'Informatique et des Libertés (CNIL) en cas de violation de données à caractère personnel.

- En cas de doute, le CERT-Asinhpa peut être amené à contacter l'une ou l'autre des 3 autorités cités ci-dessus, pour aider au routage de l'information.

5.1.3 Coordination

En principe, chaque membre du CERT-Asinhpa prend en charge l'analyse des évènements liés à son entité. Il/elle peut également prendre en charge l'analyse d'évènements concernant un autre membre, soit en support dudit membre, soit lorsque le membre n'a pas les ressources nécessaires pour cela.

Chaque organisme membre de l'Asinhpa dispose d'un processus d'escalade hiérarchique visant à informer la direction générale de l'organisation

5.1.4 Résolution

N/A – cette partie est gérée par les membres de l'Asinhpa, en autonomie ou avec l'aide d'un prestataire de type PRIS

5.1.5 Activités proactives

Partages de bonnes pratiques et de marqueurs (IoC)

5.1.6 Information et alertes

Analyse des vulnérabilités et communication aux intéressés.

6 Formulaire de notifications d'incidents

Tout membre de l'Asinhpa peut, en outre, déclarer un incident de sécurité ou sa suspicion au CERT-Asinhpa. Aucun formulaire particulier n'est nécessaire pour signaler des incidents de sécurité au CERT-Asinhpa.

7 Décharge de responsabilité

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

Le Président de l'Asinhpa,
Monsieur Mostafa Lassik