AGENCE DU NUMÉRIQUE EN SANTÉ

MINISTÈRE DU TRAVAIL DE LA SANTÉ ET DES SOLIDARITÉS
Liberté
Égalité
Fraternité

RFC 2350

CERT Santé

Statut : Validé | *Classification : Publique* | *Version : 1.9*

Agence du Numérique en Santé
2-10 Rue d'Oradour-sur-Glane, 75015 Paris –
75015 Paris
T. 01 58 45 32 50
esante.gouv.fr

Textes de référence

- Article L.1111-8-2 du code de la santé publique instituant l'obligation de signalement des incidents de sécurité des systèmes d'information
- Décret d'application n°2022--715 du 27 avril 2022
- Arrêté du 1er octobre 2015 portant approbation de la politique de sécurité des systèmes d'information pour les ministères chargés des affaires sociales (PSSI-MCAS)

SOMMAIRE

1 A PROPOS DE CE DOCUMENT

Ce document contient une description du CERT Santé, CERT sectoriel pour les secteurs de la santé et du médico-social, tel que préconisée par la RFC2350[1]. Il fournit les informations essentielles sur le CERT Santé, ses responsabilités et les services fournis.

1.1 Date de dernière mise à jour

- V1.9 : 03/2024 – Mars 2024.

1.2 Liste de diffusion des notifications

Il n'existe pas de liste de diffusion pour les modifications de ce document.

1.3 Lieu de distribution de ce document

La version courante de ce document est disponible sur le portail d'information du CERT Santé : https://www.cyberveille-sante.gouv.fr/sites/default/files/media/document/2024-03/CERTSant%C3%A9_RFC2350_v1.9.pdf.

1.4 Authenticité de ce document

Ce document a été signé avec la clé PGP du CERT Santé.

La clé publique du CERT Santé est disponible sur le site web du CERT Santé au lien suivant :

https://www.cyberveille-sante.gouv.fr/contact .

[1] http://www.ietf.org/rfc/rfc2350.txt

2 INFORMATIONS SUR LE CERT SANTE

2.1 Nom de l'entité

Nom complet : CERT Santé

2.2 Adresse

Agence du Numérique en Santé

CERT Santé

2-10 Rue d'Oradour-sur-Glane, 75015 Paris

France

2.3 Zone de temps

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

2.4 Numéro de téléphone

Numéro : +33 9 72 43 91 25

2.5 Numéro de fax

Sans objet / indisponible

2.6 Autre moyen de contact

Sans objet.

2.7 Adresse électronique

Si vous devez informer le CERT Santé d'un incident de cybersécurité ou d'un acte de cybermalveillance concernant le secteur santé ou médico-social, veuillez le contacter à : cyberveille@esante.gouv.fr .

2.8 Clé publique et information sur le chiffrement

Le CERT Santé a une clé PGP :

- Identifiant de clé : cyberveille@esante.gouv.fr
- Empreinte : 749A A628 2411 F695 5249 74D3 9F06 A162 8E92 D7E3
- https://pgp.circl.lu/pks/lookup?op=vindex&fingerprint=on&search=0x9F06A1628E92D7E3

2.9 Membres de l'équipe

La liste des membres de l'équipe n'est pas publiée. Elle est constituée d'experts en sécurité des systèmes d'information : analyse des vulnérabilités, forensique et tests d'intrusion. L'identité de l'un des membres du CERT Santé peut être communiquée au cas par cas selon la règle du besoin d'en connaitre.

2.10 Autres informations

Des compléments d'information sur le CERT Santé sont disponibles sur le portail cyberveille-santé : https://www.cyberveille-sante.gouv.fr/ .

2.11 Point de contact pour les acteurs de santé

Pour toute demande concernant la déclaration des incidents de cybersécurité ou le contenu du portail cyberveille-santé, le canal de communication à privilégier pour contacter le CERT Santé est d'envoyer un email à l'adresse cyberveille@esante.gouv.fr. En cas d'urgence, veuillez spécifier la balise [URGENT] dans le champ objet de votre email ou appeler au numéro 09 72 43 91 25.

Le CERT Santé assure une permanence de son service de réponse à incident en 24h/24 et 7j/7.

3 CHARTE

3.1 Ordre de mission

En application de l'article L1111-8-2 du code de la santé publique, le ministère de la santé et de la prévention a mis en place un dispositif de traitement des signalements des incidents de sécurité des systèmes d'information des établissements de santé et des établissements et services médico-sociaux.

Afin de garantir la cohérence globale en matière d'animation et de contrôle de la politique de SSI, le FSSI des ministères sociaux participe au pilotage de ce dispositif au même titre que la Délégation du Numérique en Santé en sa qualité de tutelle de l'Agence du Numérique en Santé (ANS).

L'Agence du Numérique en Santé (ANS) apporte un appui aux structures concernées ainsi qu'aux Agences Régionales de Santé (ARS), au travers d'une structure nationale d'assistance et d'appui appelée « CERT Santé ». Les principales missions du CERT Santé pour les secteurs santé et médico-social sont :

- Le traitement des signalements d'incidents de sécurité impactant les acteurs de la santé ;
- La veille sur l'actualité de la cybersécurité et la publication d'alertes sur les menaces sectorielles au travers du portail cyberveille-santé ;
- L'animation d'une communauté partageant des bonnes pratiques sur la sécurité du numérique en santé ;
- La réalisation d'audits de l'exposition sur internet des systèmes d'information.

3.2 Entités bénéficiant du service

Les établissements de santé, les organismes et services exerçant des activités de prévention, de diagnostic ou de soins, ainsi que les établissements et services médico-sociaux peuvent bénéficier des services du CERT Santé.

3.3 Support et/ou relations

Le CERT Santé fait partie de l'Agence du Numérique en Santé. Elle dispose d'un canal d'échange avec le CERT-FR.

3.4 Autorité

Le CERT Santé réalise ses activités sous l'autorité de la direction générale de l'Agence du Numérique en Santé et du Ministère du travail, de la santé et des solidarités.

4 POLITIQUES

4.1 Types d'incidents et niveau d'intervention

Le CERT Santé est le point de contact central pour les incidents de sécurité du numérique en santé.

L'appui apporté à la structure par le CERT Santé dépend du type et de la gravité de l'incident. Dans le cas d'un nombre important d'incidents à gérer, une priorisation du traitement sera effectuée en fonction de la criticité de la menace de cybersécurité, de l'offre de soins portée par la structure et de son impact avéré ou potentiel sur la prise en charge des patients.

Les services du CERT Santé sont les services réactifs et proactifs suivants :

- Service réalisé en 24h/24 et 7j/7 pour la réponse à incident et les jours ouvrés[2] de 9h à 18h pour les activités proactives;
- Information de sécurité et alertes ;
- Réception et analyse des déclarations d'incidents de sécurité ;
- Appui à la réponse aux incidents ;
- Coordination de la réponse aux incidents ;
- Veille et bulletins d'information ;
- Audit et conseil en sécurité.

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

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 de la partie nommée. Les informations fournies restent confidentielles et ne sont communiquées qu'au FSSI et à l'ARS compétente conformément à la PSSI des ministères sociaux, à l'article L.1111-8-2 du code de la santé publique et au décret d'application n°2016-1214 du 12 septembre 2016. Sous réserve d'acceptation par la ou les partie(s) concernée(s), le CERT Santé peut publier sur l'espace privé du portail cyberveille-santé 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 des incidents spécifiques.

Le CERT Santé peut être amenée à communiquer des informations au CERT-FR lorsqu'elle sollicite son appui ou lorsque cela concerne une structure référencée comme OIV ou OSE.

Les informations seront transmises en fonction de son marquage TLP et du principe de « besoin d'en connaitre ». Aucune information sensible ne sera envoyée par le CERT Santé à une autre partie sans un accord préalable du propriétaire de l'information.

Les informations sont gérées par le CERT Santé dans le respect de la PSSI des ministères sociaux.

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 CERT Santé utilise PGP ou Zed ! pour garantir la confidentialité et l'intégrité des documents échangés. PGP pourra être utilisé pour authentifier les fichiers échangés.

[2] A l'exception des jours où l'ANS est fermée pour cause de RTT.

5 SERVICES

5.1 Activités réactives

5.1.1 Réponse aux incidents

Le traitement des incidents est de la responsabilité des structures de santé. L'accompagnement et l'appui mis en place par le CERT Santé dans le cadre de leur signalement consistent à :

- Récupérer le signalement sur le portail des signalements des évènements sanitaires indésirables et notifier au déclarant sa prise en compte ;
- Proposer des mesures d'aide au traitement des incidents, 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.

5.1.2 Triage

Les actions réalisées sont les suivantes :

- Analyser et qualifier le signalement pour le compte de l'ARS compétente ;
- Escalader au FSSI, qui assure le pilotage du traitement en cas d'incident de sécurité majeur (incident de niveau « significatif ») ;
- Le cas échéant, diffuser une alerte 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 ;
    - Aux agences sanitaires dans le cas d'un incident majeur dans la prise en charge des patients ;
    - A la Commission Nationale de l'Informatique et des Libertés (CNIL) en cas de violation de données à caractère personnel.

5.1.3 Coordination

Les actions réalisées sont les suivantes :

- Le cas échéant, accompagner la structure concernée dans le traitement de l'incident de sécurité des systèmes d'information ;
- Alerter la Direction Générale de la Santé (DGS) via le Centre Opérationnel de Réception et de Régulation des Urgences Sanitaires et Sociales (CORRUSS), dans le cas d'un incident ayant ou pouvant avoir un impact sanitaire.

5.1.4 Résolution

Les actions réalisées sont les suivantes :

- Conseiller la ou les structure(s) concernée(s) sur les mesures appropriées ;
- Suivre le processus de résolution des incidents ;
- Analyser des artefacts et répondre, au cas par cas.

5.2 Activités proactives

5.2.1 Information et alertes

Le CERT Santé réalise une veille sur l'actualité de la sécurité des SI et sur les menaces propres au secteur de la santé. Elle informe et alerte les acteurs de santé et du médico-social au travers de la publication de bulletins de sécurité sur le portail cyberveille-santé et l'envoi de messages électroniques.

Le portail cyberveille-sante.gouv.fr est animé quotidiennement pour assurer la publication :

- De bulletins de sécurité sur les technologies standards (émergence de menaces, méthodologies d'attaques innovantes, nouvelles vulnérabilités) et spécifiques au secteur santé (incidents de sécurité, nouvelles vulnérabilités) ;
- D'alertes de sécurité et de recommandations pour se protéger des menaces en cours sur la page d'accueil du portail avec un flux RSS permettant d'en être informé ;
- De documents d'appui à la gestion de la sécurité et des incidents (fiches réflexes, fiches pratiques, guides de bonnes pratiques).

Le CERT Santé dispose d'une base de contacts permettant aussi d'alerter directement par message électronique les acteurs de santé et du médico-social lorsqu'il est informé d'une exploitation potentielle ou active d'une vulnérabilité critique.

5.2.2 Audit et évaluation de la sécurité

Le CERT Santé réalise des audits de cyber-surveillance : il s'agit d'un service de diagnostic de la sécurité du système d'information concernant son exposition sur Internet.

Les activités suivantes sont réalisées dans le cadre de cet audit :

- Recherche de fuites de données (fuite de code-sources, fuite de données utilisateur, etc.) et évaluation de leur pertinence ;
- Réalisation d'une cartographie des machines exposées (technologies et serveurs utilisés, configuration TLS, mise à jour corrective, etc.) afin de déterminer la surface d'attaque ;
- Recherche des vulnérabilités (machines non gérées type « shadow it » ou serveurs mal configurés), identifiants faibles/par défaut, vulnérabilités Web (Injections SQL, XSS, LFI, RFI, etc.) et évaluation de leur exploitabilité.

A l'issue de l'audit, le CERT Santé délivre un rapport destiné à la direction et au responsable de la cybersécurité. Il présente :

- Les vulnérabilités identifiées et leur niveau de criticité ;
- Les impacts en cas d'exploitation ;
- Les recommandations visant à réduire les risques identifiés.

6 FORMULAIRE DE NOTIFICATION D'INCIDENTS

La déclaration des incidents de sécurité des systèmes d'information pour les structures de santé se fait au travers du portail de signalement des évènements sanitaires indésirables dans la section « Professionnel de santé » :

https://signalement.social-sante.gouv.fr

L'accès au formulaire de déclaration ne nécessite pas d'authentification préalable.

7 DECHARGE DE RESPONSABILITE

Bien que toutes les précautions aient été prises dans l'élaboration des bulletins de sécurité, le CERT Santé ne peut être tenue responsable des erreurs ou omissions, ou des dommages pouvant résulter de l'utilisation des informations fournies dans le cadre de l'appui au traitement d'un incident ou publiées sur le portail cyberveille-santé.