TLP : GREEN

CERT KLESIA

RFC 2350

1. Références et standards

- TLP / PAP
- MITRE ATT&CK, https://attack.mitre.org/
- MITRE D3FEND, https://d3fend.mitre.org/
- STIX 2.1

2. Information

Ce document contient une description du CERT KLESIA selon le document RFC 2350[1]. Il fournit les informations essentielles concernant le CERT KLESIA, ses canaux de communication, son rôle et ses responsabilités.

1. Version du document

Version 1.0, mise à jour le 23/08/2024.

2. Liste de distribution

Il n'existe aucune liste de distribution.

3. Lieu de publication du document

La version actuelle de ce document est disponible sur demande auprès de l'équipe Sécurité opérationnelle de Klesia.

4. Authenticité du document

L'authenticité de ce document peut être confirmée sur demande auprès du CERT KLESIA.

5. Identification du document

Titre : 'CERT KLESIA RFC 2350'

Version : 1.0

Date du document : 05/07/2024

Expiration : ce document est valide jusqu'à la publication d'une nouvelle version.

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

3. Contact

1. Nom

CERT KLESIA

2. Adresse

Non disponible

3. Fuseau horaire

CET/CEST

4. Numéro de téléphone

Non disponible

5. Numéro de fax

Non disponible

6. Autre canal de communication

Non disponible

7. Adresse de courrier électronique

KRT@KLESIA.fr

8. Composition de l'équipe

Pour des raisons de confidentialité, la liste des membres de l'équipe n'est pas publiquement diffusée. Plus d'informations sont disponibles sur demande auprès du CERT KLESIA.

9. Autre information

Pas d'autre information

4. Charte

1. Mission

Le CERT KLESIA est un CERT fournissant des services de cybersécurité à KLESIA. La mission du CERT KLESIA est de lui fournir des services de prévention, réponse, investigation aux incidents cyber, ainsi qu'une priorisation des vulnérabilités et connaissance de la menace cyber.

Le mandat du CERT KLESIA est le suivant :

- Faciliter le partage de l'information et la coordination en cas d'incident au sein de KLESIA
- Empêcher ou réduire la propagation d'une menace cyber au sein de KLESIA et de son écosystème
- Organiser et permettre la mise en œuvre des capacités mutualisées de cyberdéfense au sein de KLESIA
- Informer et sensibiliser les acteurs clés de KLESIA des attaques susceptibles de menacer l'organisme
- Participer à la collecte de preuves pour soutenir des dossiers utiles au juridique

2. Circonscription

Le CERT KLESIA est composé de tous les éléments du système d'information de la société KLESIA visibles via les solutions de sécurité Microsoft et l'EDR Trend Micro : ses utilisateurs, ses systèmes, ses applications et ses réseaux.

3. Parrainage et affiliation

Le CERT KLESIA entretient des contacts avec les équipes CERT des organisations qu'il a sélectionné pour faire partie de ses cercles de confiance.

4. Autorité

Le CERT KLESIA agit sous l'autorité des membres du COMEX du groupe KLESIA.

5. Stratégie

1. Types d'incidents et niveau de support

Le CERT KLESIA s'occupe de tous type d'incidents de cybersécurité impactant son périmètre de supervision.

2. Coopération, échange et confidentialité de l'information

Le CERT KLESIA soutient la coordination opérationnelle et l'échange d'information entre CERT, CSIRT, SOC et autres entités similaires. Le CERT KLESIA estime que de telles actions sont positives pour le CERT KLESIA et les parties tierces, et peuvent aider à réaliser de manière plus efficace leur devoir ainsi que la résolution d'incidents de sécurité.

De plus, le CERT KLESIA attache une importance cruciale à la confidentialité de la donnée et au principe du besoin d'en connaitre. Le CERT KLESIA applique le protocole Traffic Light Protocol version 2.0[2]. Dès lors, les informations seront classifiées CLEAR, GREEN, AMBER, et RED.

Le CERT KLESIA opère selon le cadre légal français.

3. Communication

Le CERT KLESIA protège les informations sensibles selon les politiques et règlementations, de la France et de l'Union Européenne, auxquelles est soumis KLESIA.

Les communications sécurisées, incluant le chiffrement et l'authentification, sont réalisées en utilisant une clé PGP ou autre moyen, selon la sensibilité et le contexte.

[2] https://www.first.org/tlp/docs/tlp-v1.pdf

6. Services

Le CERT KLESIA fournit les services suivants :

1. Renseignement et gestion de la cybermenace

Le renseignement de la menace, a pour objectif de fournir l'information permettant au CERT KLESIA de pouvoir détecter, caractériser, éviter ou déjouer les cyberattaques. Pour cela, elle a pour ambition de connaitre les modes opératoires des attaques, les indicateurs de compromission qui les caractérisent, ainsi que les techniques, tactiques et procédures (TTP) des attaques.

Ce service a pour objectif :

- D'anticiper les menaces et les vulnérabilités qui pourraient conduire à des impacts majeurs
- De constituer les profils des attaquants
- De consolider les postures et stratégies de contre-mesures via MITRE Att&ck
- De fournir les informations discriminantes et détaillées, techniques ou organisationnelles, exploitables par les autres services contribuant ainsi à leurs objectifs
- De consolider la connaissance des menaces et des vulnérabilités, mais aussi des contre-mesures afin de pouvoir fournir ce savoir sur des contextes analogues

2. Veille des vulnérabilités

Le service de veille des vulnérabilités au sein du CERT réalise une veille des vulnérabilités qui pourraient avoir des impacts critiques sur le SI de KLESIA si elles étaient exploitées et identifie les plus critiques.

Ce service a pour objectif :

- D'identifier les vulnérabilités qui peuvent conduire aux impacts les plus graves dans le SI de KLESIA
- De permettre d'agir au plus tôt pour empêcher un attaquant d'exploiter des vulnérabilités
- De faire figure d'autorité pour que les vulnérabilités qui doivent être inexploitables le soient concrètement au sein du SI de KLESIA

3. Threat Hunting

Le service de Threat Hunting vise à mener une surveillance sécurité du SI en fonction d'une actualité, d'un contexte de menaces ou de vulnérabilités jugés par le CERT KLESIA comme étant d'intérêt. Ce service peut être utilisé en anticipation ou lors d'un incident afin de permettre de révéler la position d'une menace ou d'une vulnérabilité dans le SI à tout moment.

Ce service a pour objectif :

- De fournir une capacité à identifier le plus rapidement possible tout élément ou comportement pouvant révéler la présence dans le SI d'une menace ou d'une vulnérabilité

4. Gestion d'incident

Le service de gestion des incidents majeurs de cybersécurité encadre et coordonne la réponse aux incidents majeurs. Il peut également se retrouver en situation de coordination technique de la réponse lors de crises cybersécurité. Il a pour objectif de s'assurer de la cohésion et de la cohérence des actions sur l'ensemble de l'incident afin d'éviter ou de limiter l'impact le plus rapidement possible. Ce service opère en 24/7 grâce à la prestation « Guichet de réponse à incidents ».

Ce service a pour objectif :

- D'éviter ou de limiter l'impact d'un incident majeur sur les S.I. concernés
- Comprendre l'ensemble de l'incident et des contre-mesures ainsi que la raison de leur réussite ou de leur succès
- Coordonner l'ensemble des services impliqués dans l'analyse et la réponse à incident

5. Formation et sensibilisation

Le CERT KLESIA pourra enfin jouer un rôle pour informer et sensibiliser les acteurs clés de KLESIA des attaques susceptibles de menacer l'organisme. Ce service doit permettre également au CERT KLESIA de rayonner au sein de l'écosystème dont il fera partie.

Ce service a pour objectif :

- D'accompagner les équipes sécurités de KLESIA à monter en maturité par rapport aux activités du CERT
- De communiquer sur les statistiques relatives aux incidents, sur la base de leur classification
- De participer à la visibilité du CERT KLESIA auprès de ses bénéficiaires

Formulaire de déclaration d'un incident

Le CERT KLESIA encourage à déclarer les incidents en utilisant des courriels chiffrés avec les informations suivantes :

- Contact et information de l'organisation, avec, si possible, la clé PGP ;
- Un résumé de l'incident/urgence/crise ;
- La date et le type d'évènement ;
- La source de l'information ;
- Les systèmes affectés ;
- L'évaluation de l'impact ;
- Les détails des observations qui ont menées à la découverte de l'incident ;
- Les données techniques pertinentes ;
- Le TLP.

7. Clause de non-responsabilité

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

CONTACT

CERT KLESIA

Email : KRT@KLESIA.fr