Urgence Cyber région Sud

RÉGION SUD PROVENCE ALPES CÔTE D'AZUR

Soutenu par RÉPUBLIQUE FRANÇAISE Liberté Égalité Fraternité

RFC 2350

Contrôle du document				
	Prénom Nom	Fonction	Date	Signature
Rédaction	Florian Putaud	CP IDE	27/08/2020	
Validation	Pascal Ausseur	DG	06/10/2020	

Historique des révisions			
Version	Date	Auteur	Nature
V0.1	27/08/2020	FP	Création
V1.0	05/10/2020	TJ	Revu
V1.1	07/08/2023	TM	Revu
V1.2	02/10/2023	AH	Revu

Table des matières

1. À propos du présent document

1.1 Version du document

Ceci est la version 1.2, publiée le 2 octobre 2023.

1.2 Liste de distribution pour notifications

Les mises à jour sont notifiées par mail à l'ensemble des adhérents de l'association.

1.3 Publication du document

La dernière version du présent document est disponible à l'adresse suivante :

https://www.urgencecyber-regionsud.fr/a-propos/

Assurez-vous de posséder la dernière version.

1.4 Authenticité du document

Ce document a été signé avec la clé PGP d'Urgence Cyber région Sud.

La clé publique PGP, l'identification et l'empreinte digitale sont disponibles sur le site Web d'Urgence Cyber région Sud à l'adresse suivante : https://www.urgencecyber-regionsud.fr/a-propos/

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

2. Information de contact

2.1 Nom du centre

Le nom officiel du centre est « Urgence Cyber – CSIRT région Sud »

Il est souvent nommé par son nom usuel « Urgence Cyber région Sud » ou encore par son acronyme « UCRS ».

2.2 Adresse

Urgence Cyber – CSIRT Région Sud
Maison du numérique et de l'innovation
Place George Pompidou
83000 Toulon

2.3 Fuseau horaire

Le fuseau horaire de travail du centre est l'heure normale d'Europe centrale en hiver (UTC+1) et l'heure d'été d'Europe centrale en période estivale (UTC+2).

2.4 Numéro de téléphone

Numéro d'information : 04 23 36 09 30
Numéro d'urgence : 0 805 036 083

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 d'Urgence Cyber région Sud est :
contact@urgencecyber-regionsud.fr

2.8 Clé publique et informations de chiffrement

Le centre possède une clé publique PGP :

- ID utilisateur : Urgence Cyber région Sud <contact@urgencecyber-regionsud.fr>
- ID clé : 0xBE7A8CFC
- Empreinte digitale : 57EF DA36 4778 A533 AA17 89DE CA47 D118 BE7A 8CFC

La clé publique est disponible sur le site du centre à l'adresse :
https://www.urgencecyber-regionsud.fr/a-propos/

2.9 Composition de l'équipe

L'équipe est constituée d'analystes en cybersécurité.
Aucune information nominative relative aux membres du CSIRT n'est diffusée dans ce document.

2.10 Horaires de fonctionnement

Les horaires d'ouverture sont du lundi au vendredi de 09h00 à 18h00.
En dehors de ces heures les adhérents peuvent signaler leur incident auprès de l'Agence Nationale de la sécurité des Systèmes d'Information (ANSSI) dont les coordonnées figurent à l'adresse suivante :
http://www.cert.ssi.gouv.fr/contact/

Les entreprises non adhérentes peuvent déclarer leur incident auprès du site :
http://www.cybermalveillance.gouv.fr/diagnostic

2.11 Points de contact

Pour contacter le centre, il est préférable d'utiliser le mail : contact@urgencecyber-regionsud.fr

En cas d'impossibilité d'envoyer un courrier électronique, il est toujours possible de contacter le centre par téléphone pendant les horaires d'ouverture.

3. Charte

3.1 Missions

La mission première du centre est d'accompagner ses adhérents lors d'un incidents cyber et de leur apporter un soutien dans sa remédiation par :

- Une première analyse afin de déterminer la nature de l'incident, son étendue et son impact potentiel ;
- La prise des premières mesures dites de « réaction immédiate » ;
- Un accompagnement dans la sélection d'un prestataire spécialisé parmi nos partenaires labelisés ou qualifiés par l'ANSSI.

Dans un cadre plus préventif, le centre vous accompagne également dans l'établissement de mesures visant à réduire le risque d'incident de sécurité. A ce titre, les adhérents disposent des services suivants :

- Un système de veille et d'alerte sur les menaces et vulnérabilités pouvant impacter leurs systèmes d'information ;
- Un accompagnement dans l'élévation du niveau de cybersécurité ;
- Des sensibilisations collectives lors de nos conférences pluriannuelles.

3.2 Circonscription

Peuvent devenir adhérent, toute structure de type TPE, PME, ETI, collectivités territoriales et associations dont le siège social est basé dans un des départements de la région Sud.

Il est nécessaire d'adhérer préalablement à l'association « Urgence Cyber - CSIRT Région Sud » pour pouvoir bénéficier des services offerts par le centre.

Un formulaire d'inscription est disponible sur le site https://www.urgencecyber-regionsud.fr. Les informations suivantes vous seront demandées :

- La nomination d'un correspondant Urgence Cyber région Sud au sein de la structure ;
- La réponse à un questionnaire d'identification des composants du Système d'Information de la structure.

3.3 Affiliations

Urgence Cyber région Sud est un centre de réponse aux incidents cyber public. Il maintient des relations avec les CSIRT régionaux et le CERT-FR de l'ANSSI.

3.4 Autorité

Urgence Cyber région Sud est placé sous l'autorité du directoire de l'association éponyme. Il dispose du soutien de la région Sud et de l'ANSSI.

4. Politiques

4.1 Types d'incidents et niveau de support

Urgence Cyber région Sud est autorisé à coordonner et assurer un premier diagnostic de tout incident de sécurité informatique qui cible ou pourrait cibler l'un de ses adhérents.

Le niveau de support dépend du type et de la sévérité de l'incident, du type de l'adhérent, du nombre d'utilisateur affectés et des ressources du centre disponible sur le moment. En tout état de cause, le centre procèdera à une analyse dite « de premier niveau ». Cette dernière permettra alors d'évaluer rapidement l'incident signalé et de déterminer sa gravité, son impact potentiel et la manière dont il doit être traité.

Il est à noter qu'Urgence Cyber région Sud ne procèdera à aucune intervention directe sur les systèmes d'information incriminés. Il est attendu que l'adhérent fasse appel à sa propre équipe d'administrateurs système et réseau ou à son infogérant. Le cas échéant, la société prestataire sélectionnée dans le cadre de la remédiation de l'incident sera seule habilitée à intervenir.

4.2 Coopération, échanges et confidentialité de l'information

Au cœur de la gestion d'incidents cyber, la coopération et l'échange d'informations entre les parties prenantes jouent un rôle fondamental. Urgence Cyber région Sud reconnaît l'importance cruciale de partager des données pertinentes pour une réponse efficace. Cependant, il est impératif que ces échanges se déroulent en stricte conformité avec les restrictions légales et les principes éthiques. Dans le respect absolu du principe du "besoin d'en connaître", toutes les données échangées sont soumises à une anonymisation rigoureuse afin de préserver la confidentialité des parties impliquées.

De plus, il est à noter que chaque traitement d'incident fera l'objet d'un compte-rendu anonymisé qui sera transmis à l'ANSSI à des fins de retour d'expérience et de statistiques. Cette pratique vise à contribuer à l'amélioration continue de la cybersécurité nationale en permettant à l'ANSSI de tirer des enseignements des incidents passés et d'élaborer des stratégies plus efficaces de prévention et de réponse. Cependant, même

dans ce contexte, toutes les données personnelles ou sensibles sont soigneusement préservées, conformément aux réglementations en vigueur.

Enfin, il est également essentiel de noter que le centre n'a pas pour mission de transmettre directement des informations aux forces de l'ordre. Sa responsabilité principale consiste à fournir une assistance technique et à aider la victime à comprendre et à atténuer l'incident. Il est vivement conseillé à la victime de déposer une plainte auprès des autorités compétentes si elle souhaite poursuivre des actions légales à la suite de l'attaque. En agissant ainsi, la victime peut s'assurer que les autorités compétentes disposent de toutes les informations nécessaires pour enquêter et prendre les mesures appropriées.

Urgence Cyber région Sud s'engage à protéger la confidentialité des données et à orienter les victimes vers les autorités compétentes en cas de besoin, garantissant ainsi une approche équilibrée et responsable de la gestion des incidents cyber.

4.3 Communication

Compte tenu des types d'informations que le centre sera amené à traiter, le téléphone sera considéré, même sur des liaisons non chiffrées, comme suffisamment sécurisé pour être utilisé. De même, le courrier électronique sera considéré suffisant pour la transmission de données de faible sensibilité.

S'il est nécessaire d'envoyer des données hautement sensibles par e-mail, le chiffrement par clé PGP sera utilisé.
A noter, Urgence Cyber région Sud respecte le protocole de partage d'informations (TLP) comme décrit à l'adresse www.first.org/tlp/

5. Déclaration d'incident

Le centre encourage fortement l'emploi du numéro d'urgence dédié, particulièrement si la situation est critique ou urgente. L'appel sera traité directement par l'équipe d'analystes.

Il est également possible d'utiliser le formulaire de déclaration d'incident disponible sur le site web de l'association. Ce formulaire est conçu pour recueillir toutes les informations nécessaires pour une intervention. Vous pouvez y accéder à tout moment et le remplir à votre convenance.

6. Avertissements

Bien que les informations transmises dans le document aient été vérifiées, Urgence Cyber région Sud refuse toute responsabilité en cas d'erreur ou d'omission ou pour tout préjudice résultant d'information contenues dans ce document.

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