RFC2350

Contrôle du document				
	Prénom Nom	Fonction	Date	Signature
Rédaction	Florian Putaud	CP IE	27/08/2020	
Validation	Pascal Ausseur	DG	11/03/2021	

Historique des révisions			
Version	Date	Auteur	Nature
V0.1	27/08/2020	FP	Création
V1.0	05/10/2020	TJ	Revu
V1.1	11/03/2021	TJ	Validation

Table des matières

1. Information

Ce document contient une description du C2RC conformément aux spécifications RFC 2350. Il fournit des informations de base sur le C2RC, décrit ses responsabilités et services offerts.

1.1 Version de document

La version de ce document est la 1.1, publiée le 11 mars 2021.

1.2 Liste de distribution

Les modifications apportées à ce document sont notifiées par courriel à :

InterCERT-FR / réseau de Français CSIRT - www.cert.ssi.gouv.fr/csirt/intercert-fr

Veuillez envoyer des questions sur les mises à jour de l'adresse e-mail de l'équipe C2RC csirt@c2rcsud.org

1.3 Lieu de publication du document

Ce document a été signé avec la clé PGP de C2RC.
La clé publique PGP, l'identification et l'empreinte digitale sont disponibles sur le site Web du C2RC à l'adresse suivante :
https://c2rcsud.org/a-propos/

1.4 Authenticité du document

Titre : 'RFC2350 C2RC'
Version : 1.0
Date du document : 02/10/2020
SHA-256
Expiration : ce document est valide jusqu'à ce qu'il soit remplacé par une version ultérieure

2. Contacts

Cette partie décrit les moyens de communication du C2RC.

2.1 Nom

Nom officiel : Centre Ressources Régional Cyber

Nom court : C2RC

2.2 Adresse

Institut FMES

C2RC

Maison du numérique et de l'innovation

Place George Pompidou

83000 Toulon

2.3 Fuseau horaire

Heure normale d'Europe centrale (HNEC) (Central European Time, UTC+1) et heure d'été d'Europe centrale (UTC+2)

2.4 Numéro de téléphone

+33 04 94 05 55 50

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 du C2RC est : csirt@c2rcsud.org

2.8 Clé publique et informations de chiffrement

Le C2RC possède une clé publique PGP :

- ID utilisateur: CR2C <csirt@c2rcsud.org>
- ID clé: 0x E00825B5
- Empreinte digitale: 3407 F284 B36D 0EB1 5D2C E306 E4F1 9995 E008 25B5

La clé publique du C2RC peut être obtenue par l'envoi d'un courriel au C2RC mailto:csirt@c2rcsud.org ou peut être trouvée sur les serveurs de clés habituels.

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 heures ouvrées concernant le C2RC 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 :

www.cybermalveillance.gouv.fr/diagnostic

2.11 Points de contact

Il est préférable de contacter le C2RC à l'adresse CSIRT@c2rcsud.org. En cas d'impossibilité d'envoyer un courrier électronique il est possible de contacter le C2RC par téléphone en journée.

3. Charte

3.1 Missions

Le C2RC est en charge d'assurer un support auprès des entreprises de la région Sud Provence Alpes Côte d'Azur dans le domaine de la lutte informatique défensive (cyberdéfense) en liaison avec les organismes d'État en charge de ces sujets. Les missions du C2RC sont :

- Assurer une veille à partir de l'écosystème sécurité informatique régional et national sur les menaces et les vulnérabilités ;
- Sensibiliser les entreprises de la région de manière permanente en relayant par mail les informations disponibles auprès des organismes d'état et d'entreprises spécialisées en cybersécurité ;
- Alerter par mail ses adhérents à partir d'un maillage des organismes en charge de cybersécurité et des remontées d'informations des entreprises de la région Sud Provence-Alpes-Côte-d'Azur sur des menaces et vulnérabilités ;
- Accompagner ses adhérents victimes d'un incident informatique et les orienter vers des prestataires en sécurité informatique, référencés de la région.

3.2 Circonscription

La circonscription est composée de l'ensemble des entreprises de taille TPE, PME et ETI dont le siège social est basé dans un des départements de la région Sud Provence Alpes Côte d'Azur. Il est nécessaire d'adhérer préalablement aux services du C2RC. Un formulaire de contact est disponible sur le site www.c2rcsud.org/a-propos/ pour en faire la demande. Les informations nécessaires à l'adhésion sont :

- la nomination d'un correspondant C2RC au sein de la PME,
- la réponse à un questionnaire d'identification des composants du Système d'Information de l'entreprise

Le C2RC assure les services d'alerte et de réponse à l'incident pour l'ensemble des entreprises qui auront préalablement adhérées au C2RC. Une inscription préalable aux services du C2RC est nécessaire afin de disposer des services d'assistance.

3.3 Parrainage

Le C2RC est un CSIRT public. Il maintient des relations avec les différents CERT et CSIRT en France et en Europe.

3.4 Autorité

Le C2RC est placé sous l'autorité de l'association loi 1901, Institut FMES - Fondation Méditerranéenne d'Etudes Stratégiques (www.fmes-france.org) représenté par son Directeur Général. C'est un acteur associatif dont une partie de son financement est assuré par la région Sud, Provence-Alpes-Côte d'Azur.

4. Politiques

4.1 Types d'incidents et niveau de support

Le C2RC est autorisé à coordonner et assurer un premier diagnostic de tout incident de sécurité informatique qui cible ou pourrait cibler un de ses adhérents. En fonction de la nature de l'incident, le C2RC propose une liste de prestataire en Cybersécurité, susceptible d'aider l'entreprise dans la résolution de l'incident. Un suivi de la résolution de l'incident est assuré afin de statistiques et de capitalisation, et pour améliorer nos capacités de diagnostic.

Le niveau de support offert par le C2RC peut varier en fonction du type d'incident, de sa criticité, et des ressources disponibles pour le prendre en charge. Dans le cas ou l'incident concerne une entreprise non-adhérente du C2RC, une qualification via le service de http://www.cybermalveillance.gouv.fr sera réalisé.

4.2 Coopération, échanges, et confidentialité de l'information

Le C2RC échangera toutes les informations nécessaires avec les autres CERT/CSIRT susceptibles d'être concernés selon le besoin d'en connaître. Le partage d'information se fera dans le respect des différentes règlementations de protection existantes et respectera le CSIRT Code of Practice (www.trusted-introducer.org/TI-CCoP.pdf)

Les renseignements généraux relatifs aux incidents, tels que les noms et les détails techniques, ne sont pas publiés sans l'accord des parties désignées. S'il n'est pas convenu autrement, les renseignements fournis restent confidentiels. Le C2RC ne transmets jamais d'informations à des tiers à moins que la loi ne l'exige.

Par conséquent, ces informations peuvent être transmises partiellement à des entités telles que :

- Les partis concernés dans notre circonscription ;
- Les groupes de coopération CERT/CSIRT.

Toutes les informations sont transmises en fonction de sa classification et du principe du besoin de savoir. Seuls les extraits spécifiquement pertinents et anonymisés sont transmis. Le C2RC traite l'information dans des environnements physiques et techniques sécurisés conformément aux réglementations existantes en matière de protection de l'information.

4.3 Communication

Le C2RC respecte le protocole de partage d'informations (TLP) comme décrit à l'adresse www.first.org/tlp/.

S'il n'est pas considéré comme sûr, un courrier électronique non chiffré sera considéré comme suffisant dans le cadre de transmission d'information non sensible.

L'échange d'information sensible par courrier électronique se fera de façon chiffrée via PGP. Les mêmes règles s'appliquent aux transferts de fichiers.

5. Services

5.1 Réponse à l'incident

Le C2RC propose les services suivants dans le cadre de la réponse à l'incident de sécurité informatique :

- Réception des signalements d'incident ;
- Diagnostic de l'incident ;
- Mise en relation vers des prestataires spécialisés ;
- Compte rendu d'intervention concernant le traitement de l'incident ;
- Capitalisation de la connaissance.

5.2 Alertes et Cyberthreat Intelligence

Afin d'adapter ses capacités de diagnostic, Le C2RC réalise une veille active sur :

- La collecte de connaissances sur les acteurs de la cybermenace ;
- Les menaces, les vulnérabilités, les scénarios d'attaques et les mesures de sécurité nécessaires.

Le C2RC assure aussi une sensibilisation et une une communication de ces informations, par courriel et publication sur son site Web, sous une forme appropriée à la compréhension des entreprises.

6. Formulaire de déclaration d'incident

Nous vous remercions de signaler l'incident par courrier électronique à l'adresse csirt@c2rcsud.org

Les adhérents aux services du C2RC disposent d'un formulaire obtenu lors de l'adhésion pour signaler les incidents de sécurité. Les entreprises non adhérentes au C2RC indiqueront le nom d'une contact, son téléphone et l'objet de l'appel.

7. Avertissements

Bien que les informations transmises dans le document aient été vérifiées, le C2RC 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.