CYBER RÉUNION

CSIRT LA RÉUNION | COMPUTER SECURITY INCIDENT RESPONSE TEAM

RFC 2350

Version 1.1 – 06-11-2024

1. A propos du document

Ce document contient une description du service de réponse à incident « CSIRT La Réunion » établi selon la RFC2350[1]. Il décrit la composition de l'équipe, les services proposés et les moyens de contacts du « CSIRT La Réunion ».

1.1. Liste de distribution pour les modifications

Les modifications apportées à ce document sont notifiées :

- Au CERT-FR – https://www.cert.ssi.gouv.fr/
- À l'InterCERT France / réseau des CSIRTs français – https://www.intercertfrance.fr/
- À l'ENISA – https://www.enisa.europa.eu/
- Aux membres du réseau des CSIRT de l'UE – https://www.csirtsnetwork.eu/
- Au FIRST – https://www.first.org/
- À la Task Force CSIRT (TF-CSIRT) – https://www.trusted-introducer.org/
- Au webmaster du site CSIRT.FR – https://csirt.fr/

Veuillez adresser vos questions sur les mises à jour de ce document à l'adresse électronique du CSIRT La Réunion : csirt@cyber-reunion.fr

1.2. Ou trouver ce document

La version actuelle et la plus récente de ce document est disponible sur le site web du CSIRT La Réunion à l'adresse suivante : https://www.cyber-reunion.fr/rfc-2350

1.3. Authenticité du document

Ce document a été signé avec la clé PGP du CSIRT La Réunion.

La clé publique PGP est disponible sur le site web du CSIRT La Réunion à l'adresse suivante : https://www.cyber-reunion.fr/cle-pgp

La signature est disponible sur le site web du CSIRT La Réunion à l'adresse suivante : https://www.cyber-reunion.fr/wp-content/uploads/CSIRT-LR_RFC2350_FR.pdf.sig

1.4. Identification du document

Titre : RFC 2350 du CSIRT La Réunion
Version :1.1
Date de mise à jour : 06/11/2024
SHA 256 : voir https://www.cyber-reunion.fr/wp-content/uploads/CSIRT-LR_RFC_2350_FR.pdf.sha256.txt
Durée de validité : Ce document constitue la dernière version à jour

[1] https://datatracker.ietf.org/doc/html/rfc2350

2. Informations de contact

2.1. Nom de l'équipe

Nom complet : CSIRT La Réunion

2.2. Adresse

CSIRT La Réunion
Hébergé chez Réunion THD
Immeuble Emile Hugot
1 rue Emile Hugot Technopole
97490 Sainte-Clotilde

2.3. Zone horaire

UTC +4

2.4. Numéro de téléphone

0262.974.999 depuis La Réunion – +262.2.62.974.999 depuis l'étranger

2.5. Numéro de fax

Non applicable

2.6. Autres moyens de communication

Afin de faciliter la prise de contact, nous permettons à nos bénéficiaires de nous contacter via la messagerie instantanée « WhatsApp »[2] au numéro suivant : +262.6.92.69.17.47
A l'issue de cette prise de contact, nous les accompagnons pour échanger sur un support de communication sécurisée.

2.7. Adresse courriel

csirt@cyber-reunion.fr

2.8. Clé publique et informations liées au chiffrement

PGP est utilisé pour garantir la confidentialité et l'intégrité des échanges avec le CSIRT La Réunion avec les bénéficiaires et/ou les correspondants qui l'utilisent.
Identifiant utilisateur : csirt@cyber-reunion.fr
Identifiant de la clé : 4A3C A7BA D03F 8669

[2] https://www.whatsapp.com/?lang=fr_FR

Empreinte : 18EB0123C3FC005777EFC54F11A2545BA1FBB5EA

La clé PGP publique est disponible à cette adresse : https://www.cyber-reunion.fr/cle-pgp

2.9. Membres de l'équipe

L'équipe du CSIRT La Réunion est composée de spécialistes en cybersécurité. Pour des raisons de confidentialité, les noms des membres de l'équipe ne sont pas rendus publics. Veuillez contacter directement le CSIRT La Réunion pour de plus amples informations.

2.10. Horaires de fonctionnement

Les services du CSIRT sont ouverts du lundi au vendredi de 9H00 à 12H00 et de 13H00 à 17H00 (hors jours fériés). Fuseau horaire : UTC +4

2.11. Autres informations de contacts

Aucune à ce jour.

2.12. Contact

Pour joindre le CSIRT La Réunion, les moyens de communication à privilégier sont :

- Le téléphone au 02 62 974 999
- Le courriel à l'adresse csirt@cyber-reunion.fr
- Le formulaire prévu à cet effet sur le site internet https://www.cyber-reunion.fr/csirt/

Nous encourageons l'utilisation de chiffrement avec les informations présentées dans le paragraphe *2.8 Clé publique et informations liées au chiffrement* pour assurer l'intégrité et la confidentialité des échanges.

3. Charte

3.1. Ordre de mission

Le CSIRT La Réunion est l'équipe de réponse aux incidents établie au sein de la Régie REUNION THD. Mandaté par la Région Réunion, son objectif consiste à apporter une assistance aux organisations victimes d'un cyberattaque appelées « bénéficiaires ».

3.2. Bénéficiaires

Les entités pouvant bénéficier de l'accompagnement du CSIRT La Réunion sont les organisations localisées sur le territoire de la région La Réunion comprenant :

- Les très petites entreprises (TPE) ;

- Les petites et moyennes entreprises (PME) ;
- Les entreprises de taille intermédiaire (ETI) ;
- Les collectivités territoriales et les établissements publiques associés ;
- Les associations.

Les secteurs suivants, couverts par des CERT sectoriels, sont exclus du champ de compétences du CSIRT La Réunion. Cependant le CSIRT La Réunion peut servir de relai ou faciliter l'établissement de relation avec eux :

- La santé ;
- Le maritime ;
- L'aviation civile ;
- L'enseignement supérieur et la recherche ;
- La défense et l'armement.

3.3. Affiliation

Le CSIRT La Réunion est affilié à la Région Réunion.

3.4. Autorité

Le CSIRT La Réunion réalise ses activités sous l'autorité du directeur général de Réunion THD.

4. Politiques

4.1. Types d'incidents et niveau d'intervention

Le périmètre d'action du CSIRT La Réunion couvre tous les incidents de sécurité des systèmes d'information touchant les organisations de son territoire décrites dans le paragraphe 3.2 *Bénéficiaires*.

Les missions principales du CSIRT La Réunion consistent à :

- Offrir une réponse de premier niveau pour les incidents cyber survenant chez ses bénéficiaires ;
- Rediriger ses bénéficiaires vers des prestataires régionaux pour la remédiation de l'incident ;
- Assurer des conseils en gestion de crise à un niveau stratégique en complément de la réponse à incident ;
- Mener de la recherche de données en source ouverte dans le cadre d'une réponse à incident ;
- Mener des campagnes de détection de vulnérabilités ;
- Agir comme un relai entre les bénéficiaires et différents interlocuteurs tels que le CERT-FR, les prestataires régionaux, les services de police et de gendarmerie ;
- Consolider les statistiques d'incidentologie à l'échelle régionale ;
- Produire et diffuser des rapports réguliers sur l'état de la menace.

4.2. Coopération, interaction et partage d'information

Les informations relatives à un incident telles que le nom de la structure et les détails techniques ne sont ni publiées, ni partagées sans l'accord du bénéficiaire.

Le CSIRT La Réunion peut être amené à communiquer des informations aux autres CSIRT régionaux ou au CERT-FR lorsqu'une structure sollicite leur appui. De la même manière, des informations pourront être partagées à un CSIRT sectoriel (santé, maritime…).

La diffusion d'information sera traitée conformément au protocole Traffic Light Protocole (TLP) défini par le Forum of Incident Response and Security Teams (FIRST)[3] pour la diffusion des informations et au protocole Permissible Actions Protocol (PAP) détaillé sur le site de l'ANSSI[4] pour l'utilisation des informations.

4.3. Communication et authentification

Le CSIRT La Réunion recommande fortement l'utilisation de canaux de communication sécurisés et du chiffrement PGP, en particulier pour communiquer des informations confidentielles ou sensibles.

En matière de communication sécurisée, le CSIRT La Réunion a fait les choix d'utiliser :

- L'outil BlueFiles[5] pour transmettre les données sensibles ;
- PGP pour signer/chiffrer les courriels sensibles.

Les informations non confidentielles ou non sensibles peuvent être transmises via des courriels non chiffrés.

5. Services

5.1. Réponse aux incidents

L'activité principale du CSIRT La Réunion consiste à venir en aide à ses bénéficiaires en proposant un service de réponse de premier niveau aux incidents cyber et de les aider à poursuivre ce traitement auprès de prestataire référencés et qualifiés pour les accompagner.

En particulier, il propose les services détaillés dans les paragraphes suivants.

5.2. Triage

- Récupération du signalement et prise de contact avec le déclarant ;
- Collecte d'informations sur l'incident et confirmation ou évaluation de la nature de l'incident ;
- Détermination de la sévérité de l'incident, de son impact et de son périmètre

[3] https://www.first.org/tlp/
[4] https://www.cert.ssi.gouv.fr/csirt/politique-partage/
[5] https://bluefiles.com/fr

(ampleur quantitative de l'incident du point de vue périmètre informatique) ;
- Catégorisation de l'incident.

5.3. Coordination

- Identification d'une liste de prestataires de réponse aux incidents de cybersécurité locaux et référencés pour accompagner le demandeur ;
- Accompagnement dans la diffusion, le cas échéant, de signalements vers les autorités compétentes de l'Etat selon la nature de l'incident. Notamment, mais de manière non exhaustive :
    - › A l'ANSSI en cas d'incident majeur de cybersécurité pouvant impacter d'autres secteurs ;
    - › A la Commission Nationale de l'Informatique et des Libertés (CNIL) en cas de violation de données à caractère personnel.

5.4. Résolution

- Proposition d'actions réflexes, notamment des mesures d'urgence pour limiter l'impact de l'incident ou des mesures destinées à limiter une propagation de l'incident ou à faciliter les investigations et le traitement de l'incident ;
- Conseils en gestion de crise à un niveau stratégique en complément de la réponse à incident ;
- Recherche de données en source ouverte en appui d'une réponse à incident ;
- Partage d'une liste restreinte de prestataires référencés et qualifiés de proximité capables d'assurer la résolution et la remédiation de l'incident ;
- Suivi des phases de résolution et de remédiation.

La conduite d'opération ne fait pas partie des services délivrés par le CSIRT La Réunion.

5.5. Scans de vulnérabilité sur surface d'attaque externe

Le CSIRT La Réunion a aussi pour objectif d'évaluer la surface d'attaque du territoire réunionnais et s'emploie à réduire le nombre d'équipements vulnérables susceptibles d'être exploités par des attaquants.

A cet effet, il réalise des sondages de vulnérabilités – aussi appelés scans de vulnérabilités – sur le périmètre régional.

Ainsi, seuls les numéros « Autonomous System » (AS) des opérateurs réunionnais et les noms de domaine ayant pour TLD « .re » font l'objet de ces scans de vulnérabilités par défaut.

Ce service est exécuté de la manière suivante :

- Identification des AS et des noms de domaines cibles ;
- Scan des services hébergés sur ces domaines (et sous-domaines) et exposés sur internet ;
- Première communication synthétique auprès des entités concernées par une vulnérabilité ;
- Après retour de l'entité concernée, transmission du rapport de scan détaillant la/les vulnérabilité(s) et les recommandations associées ;
- Suivi de la remédiation sous la forme de sondages ultérieurs pour vérifier son

efficacité.

5.6. Recherche en source ouverte

Dans le cadre du suivi des incidents et de la communication avec des bénéficiaires victimes de fuites d'informations, notamment des cas de rançongiciels, le CSIRT La Réunion mène une veille en source ouverte et leur communiquera les éléments collectés dans le respect de la législation.

6. Décharge de responsabilité

Bien que toutes les précautions soient prises dans la préparation des informations, notifications et alertes, le CSIRT La Réunion n'assume aucune responsabilité pour les erreurs ou omissions, ou pour les dommages résultant de l'utilisation des informations transmises aux bénéficiaires dans le cadre de ses activités.