RFC 2350

Contrôle du document			
	Entité	**Fonction**	**Date**
Rédaction	Région Ile de France	Directeur Projet	23/09/2023
Approbation	Région Ile de France	RSSI de la Région	13/06/2024

Historique			
Version	**Date**	**Auteur**	**Nature**
V1	13/06/2024	Consultant SI IDF	Création
V1.1	06/12/2024	Consultant SI IDF	Ajout de la clé PGP Public

Région Île-de-France 2, rue Simone Veil - 93400 Saint-Ouen

Région îledeFrance
POUR GAGNER ensemble

SOMMAIRE

1. A propos du document

Ce document contient une description du CSIRT URGENCE CYBER Île de France tel que recommandé par la RFC2350. Il présente des informations sur l'équipe, les services proposés et les moyens de contacter le CSIRT régional de l'Ile de France.

1.1 Date de dernière mise à jour

Ceci est la version 1.1 de ce document, éditée le 06/12/2024

1.2 Liste de distribution pour les modifications

Toutes les modifications apportées à ce document seront partagées via les canaux suivants :

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

Veuillez envoyer des questions sur les mises à jour sur l'adresse e-mail de l'équipe CSIRT URGENCE CYBER Île de France : urgencecyber@iledefrance.fr

1.3 Où trouver ce document

Ce document peut être trouvé sur le site du CSIRT régional de l'Ile de France : urgencecyber.iledefrance.fr/files/rfc2350.pdf

1.4 Authenticité du document

Ce document a été validé par le RSSI du Conseil Régional Île de France

1.5 Identification du document

Titre : RFC 2350 du CSIRT régional de l'Ile de France.

Version : 1.1

Date de mise à jour : 06/12/2024

Durée de validité : ce document est valide tant qu'il n'existe pas de version ultérieure.

2. Informations de contact

2.1 Nom de l'équipe

Nom court : URGENCE CYBER
Nom complet : CSIRT URGENCE CYBER Île De France

2.2 Adresse

Plateau CSIRT Urgence Cyber, DCS EASYWARE Paris,
1 boulevard Hippolyte Marquès - Immeuble Métrosud,
94200 Ivry-sur-Seine

2.3 Zone horaire

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

2.4 Numéro de téléphone

0800 730 647

2.5 Numéro de Fax

Sans objet / Indisponible

2.6 Autres moyens de communication

urgencecyber.iledefrance.fr Pour le site internet

2.7 Adresse E-Mail

urgencecyber@iledefrance.fr

2.8 Clé publique et informations liées au chiffrement

ID Utilisateur : Urgence Cyber <urgencecyber@iledefrance.fr>

Empreinte : 47140CAFAA86644224D8B5D553D52EAB6CC6AB03

La clé PGP est disponible : urgencecyber.iledefrance.fr/uploads/public_key_2024.asc

2.9 Membres de l'équipe

L'équipe est constituée de 4 personnes dédiées :

- Un responsable du CSIRT ;
- Deux analystes ;
- Un chargé de communication

L'équipe est renforcée par des profils complémentaires en cas de besoin.

Aucune information nominative relative aux membres du CSIRT n'est diffusée dans ce document.

2.10 Autres informations

Des compléments d'information sur le CSIRT sont disponibles sur le portail https://urgencecyber.iledefrance.fr

2.11 Contact

Le CSIRT URGENCE CYBER Île de France est disponible par téléphone du lundi au vendredi de 8h à 18h. Pour joindre le CSIRT URGENCE CYBER Île de France, le moyen de communication privilégié est le téléphone.

Le CSIRT URGENCE CYBER Île de France aussi joignable par email en cas de surcharge d'appel ou de fermeture par l'adresse urgencecyber@iledefrance.fr

En dehors de ces heures les bénéficiaires 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/, ou bien auprès du site : www.cybermalveillance.gouv.fr/diagnostic

Nous encourageons l'utilisation de bluefiles pour assurer l'intégrité et la confidentialité des échanges.

3. Charte

3.1 Ordre de mission

Le CSIRT URGENCE CYBER Île de France est l'équipe de réponse aux incidents de sécurité informatique de la région Ile de France. Son objectif est d'apporter une assistance aux organisations de son territoire (décrites dans le paragraphe 3.2 *Bénéficiaires*) pour répondre aux incidents cyber auxquels elles font face.

Les missions du CSIRT URGENCE CYBER Île de France sont :

- Accompagner les bénéficiaires du dispositif (§ 3.2) victimes d'un incident informatique et les orienter vers des prestataires en sécurité informatique, référencés de la région
- Assurer une veille à partir de l'écosystème cybersécurité régional et national sur les menaces et les vulnérabilités ;
- Alerter les bénéficiaires de ces menaces et vulnérabilités ;
- Contribuer à la sensibilisation des administrations de la région de manière permanente en relayant les informations disponibles auprès des organismes d'état et d'entreprises spécialisées en cybersécurité.

3.2 Bénéficiaires

Les entités pouvant bénéficier de l'accompagnement du CSIRT URGENCE CYBER Île de France sont les organisations localisées sur le territoire de la région Ile de France, appartenant aux catégories suivantes :

- Les PME ;
- Les ETI ;
- Les établissements publics
- Les associations

3.3 Affiliation

Ce CSIRT est opéré par une équipe dédiée de la société DCS Easyware sous contrat avec la Région Ile de France

3.4 Autorité

Le CSIRT URGENCE CYBER Île de France réalise ses activités sous le contrôle de la Région Île de France et par contrat de sous traitance avec DCS Easyware.

4. Politiques

4.1 Types d'incidents et niveau d'intervention

Le périmètre d'action du CSIRT URGENCE CYBER Île de France décrites dans le paragraphe 3.2 *Bénéficiaires*.

Les missions principales du CSIRT URGENCE CYBER Île de France sont :

- Référencer les CSIRT N2 du territoire
- Recevoir les appels des éventuelles victimes de cyber attaque et traiter les mails.
- Qualifier les incidents et mettre en relation avec un CSIRT N2
- Communiquer les gestes de « premier secours »
- Suivre les incidents avec les bénéficiaires et les CSIRT N2
- Conseiller sur la déclaration d'incident
- Effectuer un suivi après-crise
- Consolider l'incidentologie de la Région.

Le CSIRT URGENCE CYBER Île de France autorisé à coordonner et assurer un premier diagnostic de tout incident de sécurité informatique qui cible ou pourrait cibler un de ses bénéficiaires. En fonction de la nature de l'incident, le CSIRT URGENCE CYBER Île de France propose une liste de prestataire en Cybersécurité, susceptible d'aider le bénéficiaire 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 les capacités de diagnostic.

Le niveau de support offert par le CSIRT URGENCE CYBER Île de France peut varier en fonction du type d'incident, de sa criticité, et des ressources disponibles pour le prendre en charge. Dans le cas où l'incident concerne une structure non bénéficiaire, celle-ci pourra être redirigée vers d'autres centres de réponse à incident : ANSSI, Cybermalveillance, CSIRT sectoriel…

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 pas publiées sans l'accord de la partie nommée.

Le CSIRT URGENCE CYBER Île de France 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…) à des fins de capitalisation des incidents propres au secteur concerné.

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

4.3 Communication et authentification

Le CSIRT URGENCE CYBER Île de France conseille fortement l'utilisation de canaux de communication sécurisés, en particulier pour communiquer des informations confidentielles ou sensibles. Les informations non confidentielles ou sensibles peuvent être transmises via des courriels non chiffrés.

5. Services

5.1 Réponse aux incidents

L'activité principale du CSIRT URGENCE CYBER Île de France de venir en aide à ses bénéficiaires en proposant un service de réponse de premier niveau aux incidents cyber et de les aider à affiner leur choix de prestataire pour les accompagner dans la suite de la résolution des incidents. En particulier, il propose les services détaillés dans les paragraphes suivants.

5.1.1 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 (son impact) et de son périmètre (nombre de machines affectés) ;
- Catégorisation de l'incident.

5.1.2 Résolution

- Proposition d'actions réflexes, notamment des mesures d'urgence pour limiter l'impact de l'incident ou des mesures destinées à faciliter les investigations et le traitement de l'incident ;

- Partage d'une liste restreinte de prestataires de proximité capables d'assurer la résolution et la remédiation de l'incident ;
- Suivi des phases de résolution et de remédiation ;
- Compte rendu d'intervention concernant le traitement de l'incident et capitalisation de la connaissance

5.1.3 Coordination

- Identification du meilleur partenaire au sein du dispositif national de réponse aux incidents 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.

5.2 Activités proactives

Le CSIRT URGENCE CYBER Île de France pourra aussi proposer des services proactifs à ses bénéficiaires, notamment :

- Des services de veille ;
- Des sensibilisations et des conseils pour des acteurs publics identifiés ;
- Un bulletin de veille à destination d'abonnés.
- De la sensibilisation

5.3Audit et évaluation de la sécurité

CSIRT URGENCE CYBER Île de France réalise avec deux partenaires Board of Cyber et CybelAngel 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 et évaluation de leur exploitabilité.

A l'issue de l'audit, le CSIRT URGENCE CYBER Île de France délivre un rapport destiné à la direction et au responsable de la cybersécurité des collectivités territoriales. Il présente :

- Les vulnérabilités identifiées et leur niveau de criticité ;
- Les impacts en cas d'exploitation ;

- Les recommandations visant à réduire les risques identifiés.

5.4 Formulaire de Notification d'Incidents

La déclaration des incidents de sécurité des systèmes d'information pour les :

- PME, ETI, Etablissements publics, Associations

se fait par téléphone ou au travers du portail de signalement des évènements indésirables
https://urgencecyber.iledefrance.fr/form.html
L'accès au formulaire de déclaration ne nécessite pas d'authentification préalable.

6. Décharge de responsabilité

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