CERT-MGEN : RFC 2350

TLP : CLEAR Les informations peuvent être diffusées sans restriction. Sous réserve du contrôle des droits d'auteur.	CERT-MGEN	Version : 1.0
	RFC 2350	Date de création : 29/05/2024
	Propriétaire du document : Manager SOC	Document approuvé par : CISO MGEN

I. Suivi des versions

Version	Date	Rédacteur	Modification
1.0	29/05	Manager SOC	

II. Description du document

Ce document a pour objectif de décrire le CERT-MGEN au sens de la RFC 2350. Il fournit des informations de base sur le CERT-MGEN, il décrit ses responsabilités et missions ainsi que les moyens de communication.

1. Date de mise à jour

Version 1.0, publiée le 29/05/2024.

2. Classification

Ce document est classifié **TLP : CLEAR**

3. Liste de diffusion

Il n'existe pas de liste de diffusion des notifications pour les modifications de ce document.

4. Lieux de distribution de ce document

La version courante et à jour de ce document peut être retrouvée sur le site web du Groupe MGEN : https://www.mgen.fr/cert/ CERT-MGEN-RFC-2350-FR.pdf

5. Authentifier ce document

Ce document a été signé par la clé PGP du CERT-MGEN.

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

6. Identification du document

Titre : CERT-MGEN-RFC-2350-FR

Version : 1.0

Date du document : 29/05/2024

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

III. Contact

1. Nom de l'équipe

Le nom de l'équipe est « CERT-MGEN »

2. Adresse

MGEN Technologies

3, SQ MAX HYMANS

75015 PARIS, France

3. Fuseau horaire

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

4. Numéro de téléphone

Non disponible. Numéro d'astreinte 24/7 disponible sur demande en fonction des services.

5. Adresse de courrier électronique

cert@mgen.fr

6. Clé publique et informations de chiffrement

CERT-MGEN utilise une clé publique PGP avec les caractéristiques suivantes :

- Identifiant de la clé : 121B 0518 B93A 3C27

- Empreinte : C33E6CA002A305FD2AF85A97121B0518B93A3C27

La clé publique peut être récupérée à tout moment à partir des serveurs de clés publiques applicables tels que https://pgp.circl.lu/. La clé doit être utilisée chaque fois que des informations doivent être envoyées au CERT-MGEN de manière sécurisée. Si l'utilisation de PGP n'est pas possible, veuillez contacter le CERT-MGEN au préalable de tout envoi de données sensibles pour convenir d'un moyen de transmission de données chiffrées secondaire.

7. Composition de l'équipe

Pour des raisons de confidentialité, la liste des membres de l'équipe n'est pas publiquement diffusée. Elle est composée d'experts en détection, réponse à incident, gestion de crise, analyse forensique, gestion de vulnérabilités.

Plus d'informations sont disponibles sur demande auprès du CERT-MGEN.

8. Autres informations

Pas d'autre information.

9. Point de contact clients

La méthode principale pour contacter le CERT-MGEN est le mail : cert@mgen.fr

Un numéro d'astreinte 24/7 est disponible sur demande.

Les heures ouvrées sont les suivantes : 08 :00-18 :00 du lundi au vendredi.

IV. Charte

1. Mission

La mission du CERT-MGEN est de coordonner la réponse aux incidents de sécurité informatique pour le groupe MGEN, et pour ses clients au sein du Groupe VYV.

2. Périmètre d'intervention

Le CERT-MGEN coordonne tout incident de sécurité pouvant impliquer le groupe MGEN ou ses clients au sein du Groupe VYV.

3. Support ou relations

Le financement est assuré par le groupe MGEN.

Il entretient des contacts avec des équipes de la communauté des CSIRT en France ou à l'étranger.

4. Autorité

Le CERT-MGEN opère sous l'autorité du directeur de la Cybersécurité du Groupe MGEN.

V. Politique

5. Types d'incidents et niveau de support

Le CERT-MGEN coordonne toutes sortes d'incidents de sécurité qui surviennent ou menacent de se produire au sein du périmètre du groupe.

6. Coopération, échange et confidentialité de l'information

Le CERT-MGEN échangera toutes les informations nécessaires avec d'autres CERT ainsi qu'avec d'autres parties concernées si elles sont impliquées dans l'incident ou dans le processus de réponse à incident.

Le CERT utilise le protocole « TLP » version 2.0, pour définir la confidentialité des informations.

7. Communication et authentification

Tous les courriels contenant des informations confidentielles doivent être chiffrés et signés à l'aide de PGP ou d'outils approuvés par l'ANSSI.

Les informations reçues sous forme chiffrées ne doivent pas être stockées de manière permanente sous forme non chiffrées.

Le CERT-MGEN prend en charge le protocole de partage d'informations (TLP) version 2.0.

VI. Services

Les services du CERT-MGEN comprennent :

- Services de détection d'incident
    - Déploiement et surveillance EDR
    - Collecte de logs, règles de détection, tableaux de bord
- Services de réponse à incident
    - Intervention d'analystes
    - Investigation / forensiques
- Conseil / assistance
    - Aide à la gestion de crise
    - Assistance technique
- Gestion des vulnérabilités
    - Scan de vulnérabilités
    - Aide à la gestion de vulnérabilités critiques

VII. Formulaire de remontée d'incident

Le CERT-MGEN ne dispose pas de formulaire concernant la remontée des incidents de sécurité. Il est recommandé de fournir dans la mesure du possible les éléments ci-dessous, par mail chiffré :

- Date / heure (time zone) de l'incident
- Personnes à contacter
- Contexte, description de l'incident
- Estimation de l'impact
- Les indicateurs déjà relevés (IP Sources, destination, ports, protocoles, …)

D'autres questions sur l'incident seront posées par le CERT-MGEN dès la première prise de contact.

VIII. Décharge de responsabilité

Le CERT-MGEN ne peut être tenu responsable des erreurs ou omissions, ou des dommages pouvant résulter de l'utilisation des informations fournies.