TLP:CLEAR

CERT GRTgaz RFC 2350

1. Informations

Ce document contient une description du CERT GRTgaz conformément à la spécification RFC 2350[1]. Il fournit des informations sur l'équipe de réponse aux incidents de sécurité de GRTgaz, décrit ses rôles et ses responsabilités.

1.1. Date de dernière mise à jour

Il s'agit de la version 1.0 publiée le 1er octobre 2022.

1.2. Liste de distribution pour les notifications

Il n'existe pas de liste de distribution pour les notifications.

1.3. Emplacement où ce document peut être trouvé

Le présent document et la dernière version de ce document peuvent être communiqués sur demande en contactant cert@grtgaz.com ou sur le site https://grtgaz.com/cert/.

1.4. Authentifier ce document

Ce document a été signé avec la clé PGP du CERT GRTgaz.
La clé PGP publique, son ID et son empreinte sont disponibles sur le site de GRTgaz à l'adresse :
https://grtgaz.com/cert/

1.5. Identification du document

Titre : CERT GRTgaz RFC 2350
Version : 1.0
Date : 2022-10-01
Expiration : Ce document est valide jusqu'à la publication d'une version plus récente.

[1] https://tools.ietf.org/html/rfc2350

TLP:CLEAR

CERT GRTgaz RFC 2350

2. Informations de contact

2.1. Nom de l'équipe

Nom : CERT GRTgaz
Nom complet : Computer Emergency Response Team of GRTgaz

2.2. Adresse

CERT GRTgaz
11 avenue de l'Europe
92270 Bois Colombes
France

2.3. Fuseau horaire

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

2.4. Numéro de téléphone

Non disponible

2.5. Numéro de fax

Non disponible

2.6. Autre moyen de télécommunication

Non disponible

2.7. Courriel

cert@grtgaz.com

2.8. Clés publiques et information de chiffrement

PGP est utilisé pour les échanges avec le CERT GRTgaz

- ID de l'utilisateur : CERT GRTgaz <cert@grtgaz.com>
- ID de la clé : F023 31F3 EA97 8364
- Empreinte : D65C 507C 6CCA 65DC FEFE 7A97 F023 31F3 EA97 8364

La clé publique est disponible à l'adresse : https://grtgaz.com/cert/

2.9. Membres de l'équipe

Le CERT GRTgaz est composé d'experts en cybersécurité dans les domaines de l'analyse, de l'investigation numérique, du forensique et de la réponse aux incidents de sécurité.
La liste des membres de l'équipe n'est pas disponible publiquement.

2.10. Heure de fonctionnement

Le CERT GRTgaz fonctionne sur un service 24/7/365.

Il peut être joint en heure ouvrée entre 8h00 et 18h00, du lundi au vendredi.
En période non-ouvrée, il peut être joint par courriel à l'adresse renseignée dans la section « Courriel ».

2.11. Points de contact client

Le CERT GRTgaz privilégie la notification d'une alerte de sécurité via courriel à l'adresse spécifiée dans la section « Courriel ».

Veuillez utiliser notre clé PGP pour s'assurer de l'intégrité et de la confidentialité des échanges. Voir section « Clés publiques et information de chiffrement ».

En cas d'urgence, veuillez ajouter le tag [URGENT] dans l'objet de votre courriel. Une réponse sera apportée en heures ouvrées.

2.12. Autres informations

Aucunes

3. Charte

3.1. Déclaration de mission

Les équipes opérationnelles de sécurité de GRTgaz traitent les aspects opérationnels permettant de mettre en œuvre la posture de sécurité de GRTgaz en maintenant et en exploitant les outils de sécurité et de gestion des identités, en contrôlant la cyber-conformité des projets, en supervisant les vulnérabilités et en opérant la réponse aux incidents de sécurité.

Le CERT de GRTgaz (CERT GRTgaz) est l'équipe responsable de la réponse aux incidents de sécurité, de l'analyse et de la priorisation de la remédiation des vulnérabilités, ainsi que de l'investigation numérique. La mission du CERT GRTgaz est d'anticiper et de centraliser la gestion des menaces cyber afin de protéger le Système d'Information de GRTgaz. Les activités du CERT GRTgaz couvrent la prévention, la détection et la réponse aux incidents de sécurité.

Les actions menées par le CERT GRTgaz sont motivées par plusieurs valeurs fondamentales :

- agir avec éthique, intégrité, honnêteté et professionnalisme,
- délivrer un service de qualité,
- répondre aux incidents de sécurité le plus efficacement possible,
- promouvoir le partage de l'information avec ses pairs selon le besoin d'en connaître.

3.2. Constituency

GRTgaz bénéficie de l'ensemble des services que peut fournir le CERT GRTgaz. Voir la section « Services ».

3.3. Sponsor et/ou affilié

Le DG de GRTgaz et le RSSI de GRTgaz sont les principaux sponsors de CERT GRTgaz.

3.4. Autorité

Le CERT GRTgaz agit sous l'autorité du Responsable de la Sécurité du Système d'Information de GRTgaz.

4. Politiques

4.1. Type d'incident de sécurité et niveau de support

Le CERT GRTgaz est habilité à traiter tous types de cyberattaques susceptibles d'impacter la confidentialité, l'intégrité ou la disponibilité des systèmes et des processus de GRTgaz.

En fonction de la nature des incidents de sécurité, CERT GRTgaz déploiera ses services qui incluent la réponse aux incidents de sécurité et l'investigation numérique. Le niveau de support apporté par le CERT GRTgaz variera en fonction de la gravité de l'incident de sécurité ou du problème de sécurité rencontré, de son impact potentiel ou avéré et des ressources disponibles de CERT GRTgaz.

4.2. Coopération, interaction et divulgation de l'information

Le CERT GRTgaz accorde une grande importance à la coordination opérationnelle et au partage de l'information entre les CSIRT, CERT, les SOC et les structures similaires, ainsi qu'avec d'autres organisations, qui peuvent l'assister à fournir ses services ou qui apportent un intérêt à CERT GRTgaz.

Le CERT GRTgaz opère dans le cadre légal français en vigueur.

4.3. Communication et authentification

Le CERT GRTgaz protège les informations sensibles conformément aux réglementations et politiques françaises et européennes en vigueur en France et dans l'Union Européenne.

En particulier, le CERT GRTgaz respecte les marquages de sensibilité définis par les sources d'information.

Le CERT GRTgaz reconnaît et supporte également le TLP (Traffic Light Protocol) FIRST version 2.0.

La sécurité des communications (qui comprend à la fois le chiffrement et l'authentification) est assurée en utilisant PGP ou tout autre moyen convenu, en fonction du niveau de sensibilité et du contexte.

5. Services

Cette section décrit les services du CERT GRTgaz.

5.1. Réponse aux incidents

5.1.1. Tri des incidents

Le CERT GRTgaz reçoit, analyse et priorise l'ensemble des incidents de cybersécurité afin de permettre un traitement et une remédiation efficaces.

5.1.1. Détection des incidents

Le CERT GRTgaz maintient, exploite et améliore les outils et services de détection afin d'assurer une détection optimale des intrusions.

5.1.2. Coordination des incidents

Le CERT GRTgaz assure la coordination des acteurs au sein de GRTgaz et, avec les intervenants extérieurs pour assurer une remédiation efficiente.

5.1.3. Résolution des incidents

Le CERT GRTgaz fournit des investigations numériques sur les systèmes compromis et conseille toutes les parties prenantes sur la façon la plus adéquate d'atténuer et d'éliminer la menace.

5.2. Activités proactives

5.2.1. Analyse des vulnérabilités

Le CERT GRTgaz reçoit, analyse et priorise les vulnérabilités logicielles affectant le Système d'Information de GRTgaz afin de permettre une remédiation rapide et efficace.

5.2.2. Test d'intrusion

Le CERT GRTgaz réalise des tests d'intrusion sur l'infrastructure de GRTgaz.

6. Formulaires de rapport d'incident

Pour signaler un incident de sécurité, veuillez fournir au CERT GRTgaz les informations suivantes :

- Résumé de l'événement : alerte/incident/crise ;
- Coordonnées de contact telles que le nom de la personne ou de l'organisation, l'adresse, le courriel, le numéro de téléphone ;
- Clé PGP si disponible;
- Adresse(s) IP, courriel(s), FQDN(s), hash de fichier, et tout autre élément technique pertinent.

Veuillez noter qu'au cas où vous souhaiteriez transmettre un courriel à CERT GRTgaz, veuillez inclure les en-têtes de messages, le corps de message et toutes les pièces jointes, dans la mesure du possible et conformément aux réglementations, politiques et législations en vigueur dans votre pays.

7. Avis de non-responsabilité

Bien que toutes les précautions soient prises dans la manipulation des informations, notifications et alertes, CERT GRTgaz n'assume aucune responsabilité pour les erreurs ou omissions, ou pour les dommages résultant de l'utilisation de ces informations.