TLP:CLEAR

CERT GRTgaz RFC 2350

1. Document Information

This document contains a description of CERT GRTgaz in accordance with RFC 2350[1] specification. It provides basic information about GRTgaz's Computer Security Incident Response Team, describes its roles and responsibilities.

1.1. Date of Last Update

This is the version 1.0 released on October 1st, 2022.

1.2. Distribution List for Notifications

There is no distribution list for notifications.

1.3. Locations where this Document May Be Found

The current and latest version of this document can be provided on demand by contacting cert@grtgaz.com or on the website https://grtgaz.com/cert/.

1.4. Authenticating this Document

This document has been signed with the PGP key of CERT GRTgaz.
The PGP public key, ID and fingerprint are available on the GRTgaz's website at:
https://grtgaz.com/cert/

1.5. Document Identification

Title: CERT GRTgaz RFC 2350
Version: 1.0
Document Date: 2022-10-01
Expiration: this document is valid until superseded by a later version.

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

TLP:CLEAR

CERT GRTgaz RFC 2350

2. Contact Information

2.1. Name of the Team

Short name: CERT GRTgaz
Full name: Computer Emergency Response Team de GRTgaz

2.2. Address

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

2.3. Time Zone

CET/CEST: Europe/Paris (GMT+01:00, and GMT+02:00 on DST)

2.4. Telephone Number

None available

2.5. Facsimile Number

None available

2.6. Other Telecommunication

None available

2.7. Electronic Mail Address

cert@grtgaz.com

2.8. Public Keys and Encryption Information

PGP is used for exchanges with CERT GRTgaz

- User ID: CERT GRTgaz <cert@grtgaz.com>
- Key ID: F023 31F3 EA97 8364
- Fingerprint: D65C 507C 6CCA 65DC FEFE 7A97 F023 31F3 EA97 8364

The public PGP key is available at: https://grtgaz.com/cert/

2.9. Team Members

CERT GRTgaz is made up of experts in cybersecurity analysis, investigation, digital forensics and incident response.
The full list of the team members is not publicly available.

2.10. Operating Hours

CERT GRTgaz operates 24/7/365 service.
It can be joined on business hours between 8:00AM to 6:00PM, from Monday to Friday.
Outside of business hours, it can be joined at by e-mail address specified in Electronic Mail Address section.

2.11. Points of Customer Contact

CERT GRTgaz prefers to receive security alert reports via e-mail at the electronic address indicated in Electronic Mail Address section.

Please use our PGP key to ensure integrity and confidentiality, see Public Keys and Encryption Information section.

In case of emergency, please specify the [URGENT] tag in the subject field in your e-mail. An answer will be given in business hours.

2.12. Other Information

None

3. Charter

3.1. Mission Statement

The operational cybersecurity team of GRTgaz handles the operational aspects allowing the security posture of GRTgaz to be put into effect by maintaining and exploiting security and identity management tools, controlling the projects' cyber-compliance, supervising vulnerabilities, and handling cyber-incidents response.

The CERT of GRTgaz (CERT GRTgaz) is the team responsible for incident response, vulnerability analysis and remediation prioritization, and digital forensics. CERT GRTgaz's mission is to anticipate and centralize the management of cyber threats in order to protect GRTgaz's IT. CERT GRTgaz's activities cover prevention, detection and response to security incidents.

The actions taken by CERT GRTgaz are driven by several key values:

- act according to the highest standards of ethics, integrity, honesty and professionalism,
- deliver a high-quality service to its constituency,
- ensure to respond to security incidents as efficiently as possible,
- foster information exchange with its peers on a need-to-know basis.

3.2. Constituency

GRTgaz benefits from the full range of services that can provide CERT GRTgaz. See Services section.

3.3. Sponsorship and/or Affiliation

The CEO of GRTgaz and the CISO of GRTgaz are the main sponsors of CERT GRTgaz.

3.4. Authority

CERT GRTgaz operates under the authority of the GRTgaz Chief Information Security Officer.

4. Policies

4.1. Types of Incidents and Level of Support

CERT GRTgaz is authorized to handle all types of cyberattacks that could hamper the confidentiality, integrity, or availability of GRTgaz's systems and processes.

Depending on the security incidents' type, CERT GRTgaz will gradually roll out its services which include cybersecurity incident response and digital forensics. The level of support given by CERT GRTgaz will vary depending on the severity of the security incident or issue, its potential or assessed impact and the available CERT GRTgaz's resources at the time.

4.2. Co-operation, Interaction and Disclosure of Information

CERT GRTgaz highly considers the paramount importance of operational coordination and information sharing between CSIRTs, CERTs, SOCs and similar actors, and also with other organizations, which may aid to deliver its services or which provide benefits to CERT GRTgaz.

CERT GRTgaz operates within the current French legal framework.

4.3. Communication and Authentication

CERT GRTgaz protects sensitive information in accordance with relevant French and European regulations and policies within France and the EU.

In particular, CERT GRTgaz respects the sensitivity markings defined by originators of information.

CERT GRTgaz also recognizes and supports the FIRST TLP (Traffic Light Protocol) version 2.0.

Communication security is achieved using PGP primarily or any other agreed means, depending on the sensitivity level and context.

5. Services

This section describes GRTgaz' CERT services.

5.1. Incident response

5.1.1. Incident Triage

CERT GRTgaz receives, analyzes and prioritizes all cybersecurity related incidents to enable effective handling and remediation.

5.1.1. Incident Detection

CERT GRTgaz maintains, operates, and improves detection tools and services to insure effective detection of intrusions.

5.1.2. Incident Coordination

CERT GRTgaz handles the coordination of actors within GRTgaz and with external parties to ensure swift remediation.

5.1.3. Incident Resolution

CERT GRTgaz provides digital forensics on compromised systems and advises all parties on the best way to mitigate and eliminate the threat.

5.2. Proactive activities

5.2.1. Vulnerability Analysis

CERT GRTgaz receives, analyzes and prioritizes software vulnerabilities affecting our IT systems to enable quick and effective remediation.

5.2.2. Penetration testing

CERT GRTgaz performs internal penetration testing on GRTgaz infrastructure.

6. Incident Reporting Forms

To report an external incident from the outside, please provide CERT GRTgaz the following details:

- summary of the event: alert/incident/crisis,
- contact details such as person or organization's name, address, email address, phone number,
- PGP key if available,
- IP or email address(es), FQDN(s), hash file, and any other relevant technical element.

Please note that in case you desire to forward any email message to CERT GRTgaz, please include all relevant email headers, bodies and any attachments if possible and as allowed by the regulations, policies and legislation under which you operate.

7. Disclaimers

While every precaution will be taken in the preparation of information, notifications, and alerts, CERT GRTgaz assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.