RFC–2350

RAISEGUARD CERT (RG-CERT)

RG-SOC-1.0

SEPTEMBRE 2023

RAISEGUARD

Table des matières

1 Preamble

1.1 About this document

This document is RAISEGUARD CERT (RG-CERT) presentation according to RFC2350.

1.2 Release date

This version RG-SOC-1.0 is released on 26th of September 2023.

1.3 Document availability

Document can be received by email by sending a request to: contact@raiseguard.net

1.4 Document identification and authentication

Title: RG-CERT_RFC2350
Version: RG-SOC-1.0
Document Date: 2023-09-26
Expiration: this document is valid until superseded by a later version

2 Contact information

2.1 Name of the team

LongName : RAISEGUARD CERT
ShortName : RG-CERT

2.2 Addresses

- Parc Technologique El Gazala 2088, ARIANA
- Immeuble Etraton, Rue Khadija Ben Arfa, Centre Urbain Nord 1082, Tunis

2.3 Email

- incdent@raiseguard.net: This email is used to report an incident to RG-CERT Team.
- contact@raiseguard.net: This email can be used to contact RG-CERT

2.4 Time Zone

GMT+1

2.5 Telephone number

- Fixe: +216 70 297 097 – Available during office hours
- Mobile: +216 98 800 300 – Available 24/7/365

2.6 Facsimile number

Not Available

2.7 Internet Website

https://raiseguard.net/rg-cert

2.8 Public keys and encryption

RG-CERT uses the following PGP public Key:
Name: CERT RAISEGUARD TEAM
ID: 6DADD4CA36CC381C
Fingerprint: D8D191ECD4B1B32CDDA06F10D7BB25565DA1B9EC

Key is available on following site:
https://pgp.circl.lu/
https://raiseguard.net/rg-cert

2.9 Team members

RG-CERT team leader is Ahmed Chabchoub
The team consists of:

- **Incident Response Specialists:** Highly skilled in rapid incident detection, analysis, and mitigation, they lead the team's response efforts during cybersecurity incidents, ensuring a swift and effective resolution.
- **Threat Intelligence Analysts:** Experts in collecting, analyzing, and disseminating up-to-date threat intelligence, they help in proactively identifying emerging threats and vulnerabilities.
- **Vulnerability Management Experts:** Specialize in identifying and assessing vulnerabilities in systems and software and provide recommendations for patching and mitigation strategies.
- **Forensic Investigators:** Experienced digital forensics experts who conduct in-depth investigations into security incidents, gather evidence, and support legal actions when required.
- **Security Awareness Trainers:** Responsible for developing training materials and conducting security awareness campaigns to improve cybersecurity practices.
- **Legal and Regulatory Compliance Advisors:** Assist in understanding and complying with relevant cybersecurity laws, regulations, and standards.

2.10 Operating Hours

Operation of RG-CERT are available 24/7/365. Average response time is around 12 hours.

3 Charter

3.1 Mission Statement

RG-CERT is an external entity which aims to assist its constituency from both private and public sector to prevent, investigate and respond to any cyber-security incident and cyber-threat that may have an impact on their activities.

3.2 Constituency

RG-CERT operates 24/7/365, providing cybersecurity support to both public and private sector organizations across Tunisia. Our constituency comprises a diverse range of businesses, government agencies, critical infrastructure providers, and non-profit organizations. We are dedicated to safeguarding their digital assets, responding to cyber threats, and enhancing overall cybersecurity resilience in Tunisia.

3.3 Affiliation / Sponsoring organization

RG-CERT is a private industrial CSIRT, owned, operated, and financed by RAISEGUARD, a SecOps as a Service Company member of Defensy Group.

3.4 Authority

RG-CERT is attached to RAISEGUARD and placed under the authority of the SOC Manager.
RG-CERT works internally in cooperation with other Defensy Group companies and departments (GRC, SOC, Pentesting, R&D, …).
RG-CERT cooperates externally with other national and international CERTs and CSIRTs.

4 Policies

4.1 Types of Incidents and Level of Support

RG-CERT will process any security incident related to its mission.
RG-CERT level of support will be adjusted to provide adapted level of answer on any threat, vulnerability, incident analysis (assessment, impact, remediation).

RG-CERT will do its reasonable efforts to provide its answer in the shortest possible delays.

4.2 Co-operation, Interaction and Disclosure of Information

Internal communication:
Security-related information is shared between the RG-CERT team and the client stakeholders.
By default, information is categorized as confidential and cannot be shared outside the team without the authorization of RG-CERT manager. A specific level of confidentiality may be assigned to the security-related information, on a case-by-case basis and subject to the applicable procedure by the client.

External communication:
By default, external communication is limited to a list of partners approved by RAISEGUARD CISO; typically, other CSIRTs and CERTs or security-oriented workgroups and governmental agencies (FIRST, ANCS, INPDP, …). Communication with other third

parties is handled on a case-by-case basis and upon the approval of both RAISEGUARD and the client CISOs.

4.3 Communication and Authentication

To contact RG-CERT, please send an email to: incident@raiseguard.net or contact@raiseguard.net.

For secured information exchange, the following PGP key can be used:
Name: CERT RAISEGUARD TEAM
ID: 6DADD4CA36CC381C
Fingerprint: D8D191ECD4B1B32CDDA06F10D7BB25565DA1B9EC

Key is available on following site:
https://pgp.circl.lu/
https://raiseguard.net/rg-cert

5 Services

RG-CERT provides services related to following aspects:

- **Incident Response:** Quickly respond to and mitigate security incidents to minimize damage and prevent further compromise. This includes coordinating with affected parties and stakeholders.
- **Threat Intelligence Sharing**: Collect and analyze cyber threat intelligence to provide timely warnings and information about emerging threats to your constituency.
- **Vulnerability Management:** Identify and assess vulnerabilities in systems and software and provide recommendations for patching or mitigation.
- **Security Awareness and Training:** Offer training and educational resources to help organizations and individuals improve their cybersecurity practices.
- **Malware Analysis:** Analyze and dissect malware samples to understand their behavior, origins, and potential impact.
- **Forensics Investigation:** Conduct digital forensics to determine the extent of a security incident, gather evidence, and support legal actions if necessary.
- **Security Incident Reporting**: Help organizations report security incidents to appropriate authorities and regulatory bodies, if required.
- **Threat Hunting:** Proactively search for signs of hidden threats or anomalies within an organization's network and systems.
- **Intrusion Detection and Prevention:** Deploy intrusion detection and prevention systems to identify and block malicious activities in real-time.
- **Security Risk Assessment:** Evaluate an organization's security posture, identify weaknesses, and provide recommendations for improvement.
- **Security Consultation:** Offer expert guidance on cybersecurity best practices, policies, and strategies tailored to an organization's needs.
- **Collaboration and Information Sharing:** Foster collaboration among various stakeholders and share threat information within the cybersecurity community.

- **Legal and Regulatory Compliance Guidance:** Help organizations understand and comply with relevant cybersecurity laws, regulations, and standards.

6 Incident Reporting Forms

No reporting form has been developed to report incidents to RG-CERT.
To report an incident to RG-CERT, please provide following information:

1. Contact details (name/email and optionally phone number).
2. Date of Incident discovery
3. Incident general description
4. Affected asset(s).
5. Technical information subject to technical and legal feasibility.

Incident reporting form is sent by email to: incident@raiseguard.net
Sensitive information can be cyphered using RG-CERT PGP key.

7 Disclaimer

RG-CERT will take all necessary precautions and apply its best competence and effort in the performance of its services. However, RG-CERT will take no responsibility for errors, omissions or damages resulting from the use of the information it provides. The services provided by RG-CERT are not designed or intended to address all matters of quality, safety, performance or condition of any product, material, services, systems or processes. RG-CERT and RAISEGUARD expressly exclude all warranties, conditions and other terms implied by statute or by law (including but not limited to any implied warranties of merchantability and fitness for purpose).All intellectual property rights in any reports, document, graphs, charts, photographs or any other material (in whatever medium) produced by RG-CERT in the performance of its services, including all rights in concepts, ideas and inventions that may arise, shall belong to RAISEGUARD SARL.

END OF DOCUMENT