National Cyber Security Authority

Rw CSIRT
Computer Security & Incident Response Team

Rw-CSIRT

RFC2350

Version 1.0 - June 2022

1. About This Document

This document contains a description of Rw-CSIRT in accordance with RFC 2350[1]. It provides basic information about Rw-CSIRT, its channels of communication, and its roles and responsibilities.

1.1. Date of Last Update

This is version 1.0, published on 30 June 2022 and updated on 13 September 2022.

1.2. Distribution List for Notifications

Rw-CSIRT does not use any distribution lists to notify about changes in this document. This document is kept up to date at the location specified in 1.3.

1.3. Where This Document May Be Found

The current and latest version of this document is available through the following link https://cyber.gov.rw/index.php?eID=dumpFile&t=f&f=328&token=9b6ee1f7301ba76a4b9ee014ddb16fa8607782cf

1.4. Authenticating This Document

This document has been digitally signed by the management of the National Cyber Security Authority, the host of Rw-CSIRT.

1.5. Document Identification

Title	**RFC 2350**
Version	1.0
Document Date	30 June 2022
Expiration	This document is valid until superseded by a later version

2. Contact Information

This section describes how to contact Rw-CSIRT.

2.1. Name of the Team

Full Name	Rwanda - Computer Security Incident Response Team
Short Name	Rw-CSIRT

[1] http://www.ietf.org/rfc/rfc2350.txt

2.2. Address

8 KG 7 St, Telecom House, Kacyiru, Kigali-Rwanda

2.3. Time Zone

GMT+2

2.4. Telephone Number

Phone: +250 781 813 310

Toll-free: 9009

2.5. Facsimile Number

N/A

2.6. Other Telecommunication

N/A

2.7. Electronic Mail Address

For notifications, incident reporting, and vulnerability reporting, please contact us at: rwcsirt@ncsa.gov.rw, incident@ncsa.gov.rw, vulnerability@ncsa.gov.rw

2.8. Public Keys and Encryption Information

Email	rwcsirt@ncsa.gov.rw
Fingerprint	AB04 23C6 6CA9 DC9E AB15 42AC 5121 B324 7512 D852
Encryption key	PGP Key
Email	incident@ncsa.gov.rw
Fingerprint	D1EF 2ECA 28BE 26A8 2670 3CF6 A90C 1076 1569 A8D0
Encryption key	PGP Key

2.9. Team Members

The list of the Rw-CSIRT team members is not publicly available. Information about the team members may be disclosed upon request.

2.10. Other Information

See our page at https://cyber.gov.rw/rw-csirt/ for additional information about Rw-CSIRT.

3. Charter

3.1. Mission Statement

The host of the Rwanda Computer Security Incident Response Team (Rw-CSIRT), the National Cyber Security Authority (NCSA), coordinates national cybersecurity functions across the private and public sectors to ensure the security and resilience of Rwanda's ICT ecosystem. NCSA also promotes national education programs, fostering awareness of cybersecurity best practices amongst the Rwandan population.

Rw-CSIRT focuses on delivering particular support to members of the public and private institutions that are affected by cyber incidents. The team releases timely alerts and advisories to foster the cyber resilience and security of the ICT infrastructure and also coordinates efforts for early detection, prevention, and response against cyber-related incidents.

3.2. Constituency

The constituencies of Rw-CSIRT are composed of all the public and private institutions in Rwanda. Constituents include:

1. Government institutions
2. Financial sector
3. Academia Sector
4. Health sector
5. Internet service providers
6. Energy sector
7. Hospitality industry

3.3. Sponsorship and /Or Affiliation

Rw-CSIRT operates under National Cyber Security Authority (NCSA).

3.4. Authority

Rw-CSIRT operates under the National Cyber Security Authority (NCSA) as one of its divisions. The power and authority of NCSA are described in article 10 of Law No 26/2017 of 31/05/2017 establishing the National Cyber Security Authority and determining its mission, organization, and functioning.

4. Policies

4.1. Types of Incidents and Level of Support

Rw-CSIRT is authorized to address all types of computer security incidents that occur or threaten to occur, in its constituencies.

The level of support delivered by Rw-CSIRT varies depending on the type and severity of the incident, the type of constituent, the size of the user community affected, and the availability of Rw-CSIRT’s resources at the time.

4.2. Cooperation, Interaction, and Disclosure of Information

All information received by Rw-CSIRT related to cyber security incidents is considered confidential and is used only to resolve incidents and prevent further potential incidents. Information that is sensitive (such as personal data or system configurations) or may be harmful, is processed in a secure environment and encrypted if it must be transmitted.

Rw-CSIRT works in cooperation with other CERT/CSIRT/SOC teams, our technological partners, administrators of the affected resource, and law enforcement institutions, on a need-to-know basis for the sole purpose of incident handling (i.e., to the extent necessary to identify and mitigate the threat). No personally identifying information is exchanged, unless explicitly authorized.

Please visit our privacy statement at https://cyber.gov.rw/privacy-policy/

4.3. Communication and Authentication

The preferred method of communication is via email.

For low sensitivity information, unencrypted methods such as emails or phones can be used.
All sensitive information shared with Rw-CSIRT should be encrypted with our PGP Public Key.

5. Services

5.1. Reactive services: are services that react to an incident situation. These services are subdivided into:

- Alerts & Warnings
- 24/7 Incident handling and response
- Vulnerability handling
- Cyber threat intelligence sharing
- Incident response coordination
- Vulnerability response coordination
- Artifact handling
- Design of countermeasures to prevent further continuation, propagation and recurrence of incidents

5.2. Proactive services: are designed to detect & prevent attacks before there is an actual impact on the production systems. In this category of services, the information generated by the Rw-CSIRT gets disseminated to their constituency and partners for protecting their assets and avoid being the target of an attack.

- Security Audits, Vulnerability assessment/Pentests
- Intrusion Detection/Intrusion Prevention and WAF services
- Endpoint protection services
- Technology Watch
- Child online protection
- Cooperation with other CIRT teams
- Security-Related Information Dissemination
- Awareness Building

5.3 Security Quality Management: services can be demanded by the constituency for review and improvement of the security posture of their organizations. This category of

services is not time-dependent and is usually demanded by the constituency which makes the request to the Rw-CSIRT.

- Risk Analysis
- Business Continuity and Disaster Recovery Planning
- Providing Cyber Security Consulting
- Education/Training

6. Incident Reporting

No specific form is needed to report security incidents via email or phone.
When reporting an incident on the NCSA website, some key information (contact, description of the incident, location etc...) are mandatory. Please visit https://cyber.gov.rw/report-incident/ for further information.

7. Disclaimer

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