BW-CIRT Description for RFC 2350

1. Document Information

1.1 Date of Last Update

This is version 1.2, published 18-03-2021

1.2 Distribution List for Notifications

BW-CIRT will not plan frequent modifications to this document, thus see clause 1.3 for the download location.

1.3 Locations where this Document May Be Found

https://www.cirt/org.bw/services

2. Contact Information

2.1 Name of the Team

BW-CIRT - Botswana Computer Incident Response Team

2.2 Address

Botswana Communications Regulatory Authority
Plot 50671 Independence Avenue
Gaborone
Botswana

2.3 Time Zone

Botswana Time is 2 hours ahead of Greenwich Mean Time (GMT+2), and is in Central Africa Time Zone (CAT)

2.4 Telephone Number

+267 3929960/1/2
+267 73048347/49/51

Backup Telephone:
+267 3685548

2.5 Facsimile Number

Not applicable

2.6 Other Telecommunication

Available upon reasonable requests - GSM, etc

2.7 Electronic Mail Address

Official Email address : Info(@)cirt.org.bw,
Email address for incident reporting : ticket(@)cirt.org.bw

2.8 Public Keys and Encryption Information

- The BW-CIRT has a PGP keyID 0xbe3be88ba4900dfd
- PGP Key Fingerprint CE8A E05F CAAF 011D 07A2 3F8A BE3B E88B A490 0DFD.
- The key and its signatures can be found at public key servers like https://pgp.circl.lu/.
- Please use this key when you want/need to encrypt messages that you send to BW-CIRT.

2.9 Team Members

The head of BW-CIRT is Emmanuel Thekiso
Information about other team members is available by request.

2.10 Other Information

- General information about BW-CIRT is available at https://www.cirt.org.bw.
- BWCIRT complies with the CSIRT Code of Practice - https://trusted-introducer.org/CCoPv21.pdf.
- BWCIRT supports the use of the Information Sharing Traffic Light Protocol (abbreviated TLP; sponsored by FIRST and TF-CSIRT) - https://www.first.org/tlp

2.11 Points of Customer Contact

- Regular Cases: the preferred method for contacting BW-CIRT is via info(@)cirt.org.bw
- Regular response Hours: from Monday to Friday, 07:30 -17:00
- Emergency Cases: If it's not possible to use e-mail, please call the official phone numbers indicated in p.2.4

3. Charter

3.1 Mission Statement

The mission of BW-CIRT is to create, maintain, and promote adequate capabilities for Botswana to respond to cyber threats and to protect its national critical information infrastructures. The goals are :-

- Act as a single point of contact for cyber incident reporting, coordination and international cooperation on cyber incidents in Botswana;
- Provide computer security incident response support at national level.
- Disseminate and share critical information such as early warnings and alert notifications, security advisory, and upholding security best practices.
- Build capacity in all the above areas using advanced technology and techniques, establishing methods, and researching threat analyses and mitigations.
- Raise awareness in the field of information security

3.2 Constituency

The BW-CIRT provides services to the Government, Communication Service Providers licensed under Communications Regulatory Authority Act, Information technology systems in the public administration and National Critical information infrastructure.

3.3 Sponsorship and/or Affiliation

- BW-CIRT is a department of the Botswana Communications Regulatory Authority (BOCRA) https://www.bocra.org.bw and is funded from the BOCRA budget. BOCRA is a Government organization under the Ministry of Transport and Communications.
- BW-CIRT is a member of AfricaCERT (https://www.africacert.org/

3.4 Authority

- BW-CIRT is department under BOCRA, and operates under the Communications Regulatory Authority Act of 2012.
- The team coordinates security incidents on behalf of their constituency and has no authority reaching further than that.
- The team is however expected to make operational, non-obligatory recommendations in the course of their work. The implementation of such recommendations is not a responsibility of the team, but solely of those to whom the recommendations were made.

4 Policies

4.1 Types of Incidents and Level of Support

- The BW-CIRT is authorized to address all types of computer security incidents which occur, or threaten to occur, in its constituency. The level of support given by BW-CIRT will vary depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected, and the BW-CIRT's resources at the time.
- Special attention will be given to issues affecting critical information infrastructure.
- No direct support will be given to end-users, as they are expected to contact their system administrators.
- BW-CIRT is committed to keep the constituency informed of potential vulnerabilities and existing threats, and where possible, will inform them of such threats and vulnerabilities before they are actively exploited.

4.2 Co-operation, Interaction and Disclosure of Information

- ALL incoming information is handled confidentially by BW-CIRT, regardless of its priority. Information that is evidently sensitive in nature is only communicated and stored in a secure environment, if necessary, using encryption technologies. When reporting an incident of sensitive nature, kindly state so explicitly, e.g., by using the label SENSITIVE in the subject field of e-mail, and if possible, using encryption as well.
- BW-CIRT supports the Information Sharing Traffic Light Protocol (see https://members.first.org/tlp/) - information that comes in with the tags WHITE, GREEN, AMBER or RED will be handled appropriately.
- BW-CIRT cooperate with other organizations like law enforcement, to protect the privacy of its constituency and stakeholders, and operates within the laws of Botswana when disclosing information.

4.3 Communication and Authentication

- For communication which does not contain sensitive or classified information, normal methods like e-mail will be used.
- For secure communication BW-CIRT PGP key will be used for encryption and signing.
- In cases where there is doubt about the authenticity of information or its source, BW-CIRT reserves the right to authenticate this by any (legal) means.

5. Services

5.1 Reactive Services

BW-CIRT is responsible for the coordination of security incidents involving its constituency (as defined in 3.2). BW_CIRT assist system administrators in handling technical and organizational aspects of incidents. It provides assistance or advice with respect to the following aspects of incident management:

- Incident response
- Cyber threat intelligence
- Alerts and Warnings
- Incident detection & resolution
- Incident analysis
- Assistance with incident handling
- Reaction to incidents
- Coordinating responses to incident handling
- Design of countermeasures to prevent further continuation, propagation and recurrence of incidents

5.2 Preventive Activities

BW-CIRT pro-actively advises its constituency regarding recent vulnerabilities and trends in hacking/cracking, and includes: -

- Education and raising awareness in the field of information security
- Provide training in incident management
- Cooperation with other CIRT teams
- Monitoring and documentation of incidents
- Receiving and sending early warnings of incidents
- Announcements about existing vulnerabilities
- Technology watch
- Information dissemination
- Threats Monitoring in the field of ICT
- Assistance with the development of new CIRT teams

6. Incident Reporting Forms

If possible, please write an email with detailed description of the incident to incident(at)csirt.sk. Link to information on how to proceed is https://www.cirt.org.bw/

7. Disclaimers

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