CERT-MU

RFC 2350 Profile

1. Document Information

1.1. Date of Last Update

This is version 1.2 published 18-09-2023

1.2. Distribution List for Notifications

CERT-MU will not plan frequent modifications to this document.

2. Contact Information

2.1. Name of the Team

Computer Emergency Response Team of Mauritius (CERT-MU)

2.2. Address

3rd Floor Wing A, Shri Atal Bihari Vajpayee Tower, Ebène, Republic of Mauritius

2.3. Time Zone

We are located in the Indian Ocean, which is

- GMT+4, between last Sunday in October and last Sunday in March
- GMT+3, between last Sunday in March and last Sunday in October

2.4. Telephone Number

Tel: +230 460-2600

Hotline: +230 800-2378

2.5. Electronic Mail Addresses

- first_rep@cert.govmu.org – Representative of FIRST
- first_team@cert.govmu.org – Team’s Representative of FIRST

- contact@cert.govmu.org – for general information
- incident@cert.govmu.org – for incident related matters
- vulnerability@cert.govmu.org – for reporting vulnerabilities

2.6. Public Keys and Encryption Information

- Email: incident@cert.govmu.org

  PGP KeyID: 37E8373C

  Fingerprint: 9587 E51E 7001 06D5 80F7 8D95 34ED 7F98 37E8 373C

- Email: first_rep@cert.govmu.org

  PGP KeyID: E858A56F

  Fingerprint: 2EE1 DA39 0952 9DE0 8165 2286 9132 18B8 E858 A56F

- Email: first_team@cert.govmu.org

  PGP KeyID: 49B316F5

  Fingerprint: F7EE F199 C05C 6D75 CE60 C26D DE98 B1DE 49B3 16F5

2.7. Team Members

The head of CERT-MU is Dr. Kaleem Ahmed Usmani. Information about other team members is available upon request.

2.8. Other Information

- General information about CERT-MU is available at:

  https://cert-mu.govmu.org/SitePages/Index.aspx

- Online system for reporting cybercrime:

  http://maucors.govmu.org/English/Pages/default.aspx

- Automated platform for sharing cyber threat intelligence information:

  https://maushield.govmu.org/misp

2.9. Points of Customer Contact

The preferred communication channel is the telephone. If it is not possible to contact the CERT-MU by using the telephone, then please use the official email addresses as mentioned in section 2.5.

3. Charter

3.1. Mission Statement

The main goals for CERT-MU, as a national CERT, are to:

- Handle security incidents and monitor security problems occurring within public and private sectors.
- Provide guidance to providers of critical information infrastructure to adopt best practices in information security.
- Warn and educate systems administrators and users about latest information security threats and suggest countermeasures by means of information dissemination.

3.2. Constituency

CERT-MU's constituency are as follows:

- The entire cyber community of Mauritius.
- CERT-MU will receive intrusions attempts reports, virus incidents and other security problems from defined staff of each constituent within each institution, namely Security Contact Person(s).

3.3. Sponsorship and/or Affiliation

CERT-MU is a national CERT which operates under the aegis of the Ministry of Information Technology, Communication and Innovation. CERT-MU is ISO 27001:2013 certified since May 2017.

CERT-MU is a member of the following:

- Forum of Incident Response and Security Teams (FIRST)
- Cybersecurity Alliance for Mutual Progress (CAMP)
- Anti-Phishing Working Group (APWG)
- CERT Coordination Centre (CERT-CC, Carnegie Mellon University)
- AfricaCERT

CERT-MU has also signed a memorandum of understanding (MoU) with Seychelles, Japan, Estonia.

3.4 Authority

CERT-MU operates under the aegis of Ministry of Information Technology, Communication and Innovation as per the Cybersecurity and Cybercrime Act 2021:

https://www.icta.mu/documents/2021/12/cybersecurity_act_2021.pdf

4. Policies

4.1. Types of Incidents and Level of Support

CERT-MU 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 CERT-MU 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 CERT-MU's resources at the time. CERT-MU will provide cooperation as soon as possible and will also provide support to its constituents. CERT-MU is also committed to keep all its constituents informed on potential vulnerabilities, and assistance to its constituents in implementing proactive measures to reduce the risks of information security incidents as well as responding to such incidents as and when they occur.

4.2. Co-operation, Interaction and Disclosure of Information

CERT-MU works in cooperation with State Institutions, Law Enforcement Organizations and professionals in the field. Standard privacy laws apply. In case of a potential criminal incident, we recommend the proper law enforcement organizations assistance. Rules and good practice are in place to avoid dissemination of private and company data.

4.3. Communication and Authentication

For international communications ordinary precautions apply, for e.g. communicating to/via previously trusted and listed/accredited teams (TI) and using PGP.

5. Services

5.1 Incident Response

CERT-MU will assist IT-security teams in handling the technical and organizational aspects of incidents. In particular, it will provide assistance or advice with respect to the following aspects of incident management:

5.1.1. Incident Triage

- Investigating whether an incident is authentic
- Assessing and prioritizing the incident

5.1.2. Incident Coordination

- Determining and contacting the involved organizations.
- Facilitating contact with other parties including law enforcement, if needed.

- Asking for reports and/or composing reports, depending on the involved organizations, incident type and severity.
- Communicating with media, if necessary.

5.1.3. Incident Resolution

- Advising the involved organization(s) on appropriate measures.
- Following up the incident solution process.
- Collecting evidence and interpreting data, if applicable.

CERT-MU will also collect statistics about incidents within its constituency.

5.2 Proactive Activities

- Issuance of Security Alerts
- Targeted alerts to critical sectors
- Organization of Security Awareness Programmes for home users and public in general
- Organizing Trainings/workshops for CIOs and System administrators
- Collaboration with Industry and International CERTs
- Assistance to Organizations in the implementation of Information Security Management Systems (ISMS) based on ISO 27001:2013 standard.
- Provide Vulnerability Scanning Service
- Provide Assistance as a third Party Auditor of Information Security Management Systems(ISMS) based on ISO 27001 standard

6. Incident Reporting Forms

- Incidents should be reported on the Mauritian Cybercrime Online Reporting System (MAUCORS) which is an online platform that allows the public to report cybercrimes
- Incidents can also be reported on the email address “incident@cert.ncb.mu” and as well as in person at CERT-MU’s office. For proof of identity, the incident reporting party should bring their Identity Card or passport (if other than Mauritian citizen).
- An incident must be reported by the victim only. In case the person may not be able to come personally, then he/she can authorize any other person, together with an authorization letter duly signed and ID card or power of attorney.
- Enquiries about incidents can be made through CERT-MU Hotline: 800 2378

7. Disclaimers

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