

CERT-MU

Computer Emergency Response Team of Mauritius

www.cert-mu.org.mu

By Reechaye Sachindra
Information Security Consultant
sreechaye@cert-mu.gov.mu



National Computer Board



CERT-MU

WORLD

LOCATION OF MAURITIUS



Copyright © 2012-13 www.mapsofworld.com
(Updated on 28th September, 2012)



National Computer Board



CERT-MU





Mauritius

- Population -1.3 M
- Diversity
- Facebook (>400k users)



Multicultural







National Computer Board

CERT-MU Mission

To enhance the security of Mauritius information and communications infrastructure through effective collaboration and communication with all stakeholders



National Computer Board



CERT-MU

CERT-MU Objectives

- Serve as a central point for responding to computer security incidents
- Create awareness on security issues through dissemination of information
- Increase awareness and understanding of information security and computer security issues
- Tracing of latest information on cyber security threats and alerting user community
- Enhancing Information Security Risk Management at national level

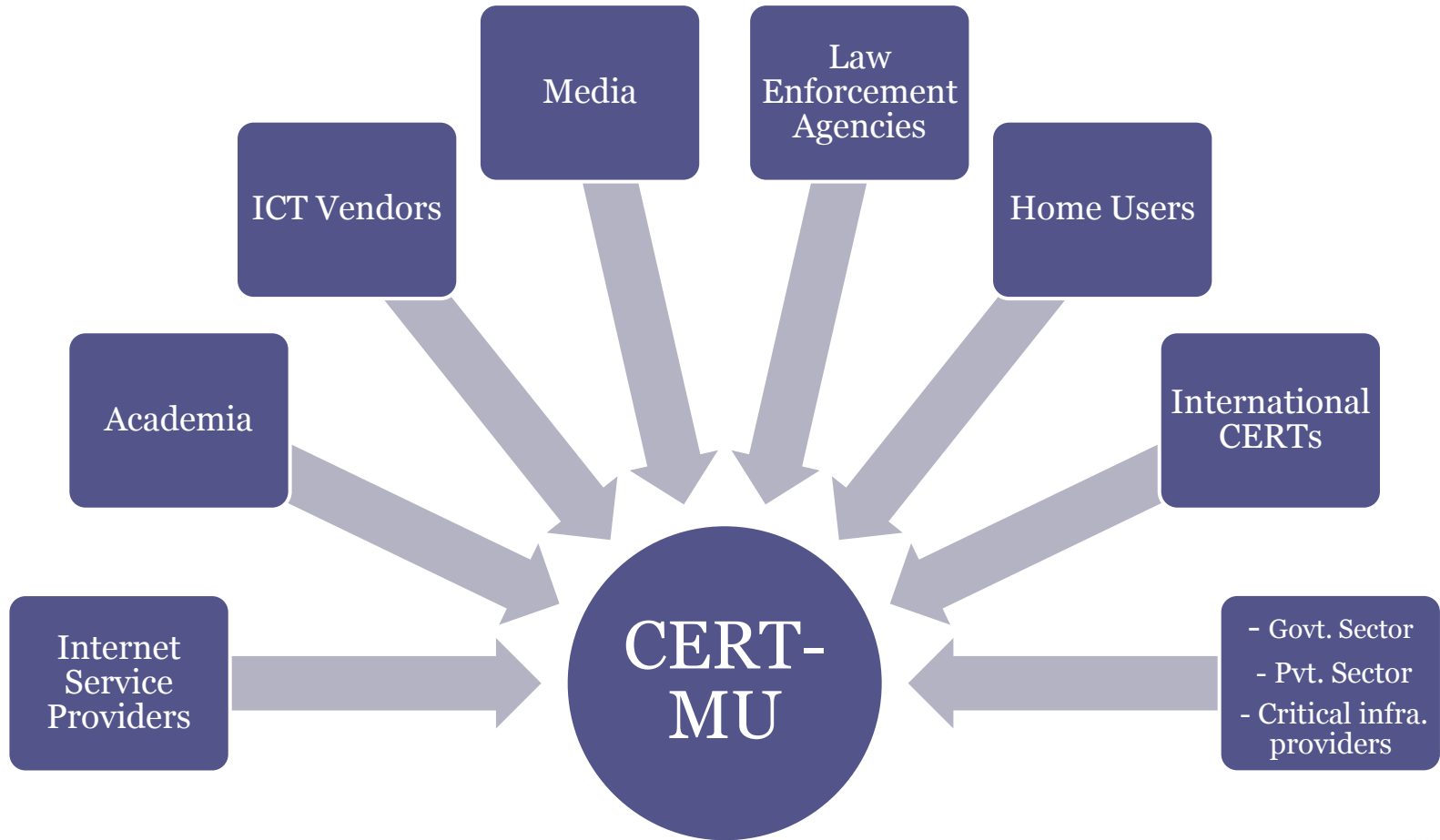


CERT-MU Services

- Incident Response and Coordination
- Vulnerability Scanning and Assessment
- Assistance in the Implementation of ISO 27001
- Information Security Audits
- Information Security Awareness
 - Technology Workshops
 - Capacity Building
 - Presentations
- Issuance of Security Alerts
 - Advisories & Vulnerability Notes
 - Virus Alerts
 - Information Security News



CERT-MU Constituency



Incident Response

- **Types**
 - Virus Infections
 - Phishing/Scam/Spam
 - Hacked Accounts
 - DOS Attacks
 - Botnets
 - Online Harassment
 - Sextortion



Vulnerability Check

- Assessing vulnerabilities of your:
 - Servers
 - Applications
 - Network Devices
 - Databases



ISO 27001

- The implementation of Information Security Management System (ISMS) based on ISO 27001 in your organisation.

We provide advice on:

- Risk Assessment
- Policies and Procedures
- Selection and Implementation of security controls
- Internal Audit Process
- Business Continuity Planning



Information Security Audit

- Third Party Information Security Audits. This will provide:
 - Auditing of information infrastructure based on ISO 27001
 - Vulnerability Scanning and Penetration Testing
 - Recommendations, reports and remedial actions on identified vulnerabilities



Awareness

- Security Awareness Programmes
 - Technology Workshops (on a quarterly basis)
 - Int. Events - Safer Internet Day & Computer Security Day
 - Capacity Building (ISO, BCM, Malware Analysis, SSD)
 - Presentations in Schools & Community Centres



Dissemination of Information Security News

- Issuance of Security Alerts
 - Advisories & Vulnerability Notes
 - Virus Alerts
 - Information Security News
 - Weekly Security Bulletin

Subscribe to CERT-MU's mailing list to receive
security alerts:

subscribe@cert-mu.gov.mu





Mauritian National Computer Security Incident Response Team (CERT-MU)



CERT-MU

Looking for SEARCH



- About CERT-MU
- CERT-MU Services
- Information Security News
- Reporting
- Knowledge Bank

Highlights

News

Events

Click here to download the National Cyber Security Strategy (draft)



< prev 1 2 3 4 5 next >



Threats RSS Feed - Symantec Corp.

- ▶ Backdoor.Lokidok
- ▶ Android.Malminer
- ▶ PUA.Maltrec.TS!g1
- ▶ Trojan.Cryptodefense
- ▶ W32.Craq
- ▶ Bloodhound.Exploit.550
- ▶ Trojan.Gampass!gen5
- ▶ Trojan.Trensil

Quick Links

Vulnerability Notes

Report All Incidents

ments/Strategy%20Doc/National%20Cyber%20Security%20Strategy.pdf in for the week of 24. March 2014 NEW



Mauritian National Computer Security Incident Response Team (CERT-MU)



CERT-MU

Looking for

SEARCH



About CERT-MU ▾

CERT-MU Services

Information Security News ▾

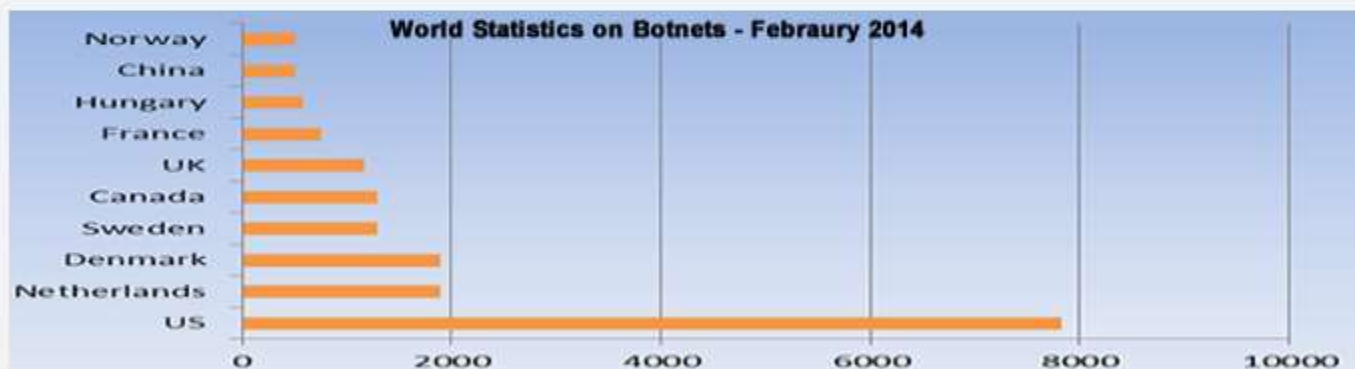
Reporting ▾

Knowledge Bank ▾

Highlights

News

Events



« prev 1 2 3 4 5 next »



Threats RSS Feed - Symantec Corp.

- ▶ Backdoor.Lokidok
- ▶ Android.Malminer
- ▶ PUA.Maltrec.TS!g1
- ▶ Trojan.Cryptodefense
- ▶ W32.Craq
- ▶ Bloodhound.Exploit.550
- ▶ Trojan.Gampass!gen5
- ▶ Trojan.Trensil

Quick Links

Vulnerability Notes

▶ CERT-MU Security Bulletin for the week of 24, March 2014 **NEW**

Report All Incidents



CERT-MU Affiliations

- **CERT –CC**
- **FIRST** – Forum of Incident & Response Security Teams
- **IMPACT** – International Multilateral Partnership Against Cyber Threats
- **APWG** – Anti-Phishing Working Group

Quick Links

- ▶ National Computer Board
- ▶ Cyber Security Portal
- ▶ Safer Internet Day
- ▶ Computer Security Day

Vulnerability Scanning



Full Member



Member



National Computer Board

Vulnerability Notes

> [CERT-MU Security Bulletin for the week of 24, March 2014](#) **NEW**

(March 28, 2014)

> [VN-2014-60](#) **NEW**

Cisco IOS SSL VPN HTTP Processing Flaw Lets Remote Users Deny Service...

(March 28, 2014)

> [VN-2014-59](#)

Cisco Unified Contact Center Express NTP Mode 7 Denial of Service Vulnerability

(March 27, 2014)

> [VN-2014-58](#)

Linux Kernel xen-netback NAPI Packet Handling Denial of Service Vulnerability

(March 26, 2014)

> [VN-2014-57](#)

Microsoft Word RTF File Processing Flaw Let Remote Users Execute Arbitrary...

(March 26, 2014)

> [VN-2014-56](#)

Nessus Malicious Process Detection Plugin Lets Local Users Gain Elevated...

(March 25, 2014)

>>More

/mu ||

Report All Incidents



For Information Security & Privacy Breaches

NATIONAL CYBER SECURITY STRATEGY



Survey



Start Now >



Subscribe to Mailing List

Get the weekly bulletin, advisories and latest alerts on Information Security

[Subscribe Now >>](#)



CERT-MU

Online Incident Reporting Form



CERT-MU
Incident Reporting Form



* are mandatory fields and need to be filled.

1. Contact Information of Reporting Party:

* Title:	<input type="text"/>	Organisation:	<input type="text"/>
* Name:	<input type="text"/>	Position/Post:	<input type="text"/>
* Address:	<input type="text"/>	Nationality:	<input type="radio"/> Mauritian <input type="radio"/> Others
		NIC :	<input type="text"/>
		* Email:	<input type="text"/>
* Telephone No:	<input type="text"/>	Fax No:	<input type="text"/>
		Mobile No:	<input type="text"/>

2. Sector of Reporting Party: *

<input type="checkbox"/> Government	<input type="checkbox"/> Financial	<input type="checkbox"/> Utilities	<input type="checkbox"/> Tourism	<input type="checkbox"/> Transportation	<input type="checkbox"/> Manufacturing
<input type="checkbox"/> Health	<input type="checkbox"/> ICT	<input type="checkbox"/> Academia	<input type="checkbox"/> Telecommunications	<input type="checkbox"/> Other	<input type="text"/>

3. Location of Affected Computer/Network:

6. Type of Incident: *

Phishing

Break - in / Root Compromise

System Misuse

Virus / Malicious Code

Spam

Social Engineering

Network Scanning / Probing

Email Spoofing

Technical Vulnerability

Web Site Defacement

Denial of Service

User Account Compromise

Intrusion

Others (Specify)

IP Spoofing

7. Description of Incident:





Knowledge Bank








- Guidelines
- e-Security Newsletter
- Weekly Security Bulletin
- Presentations
- World CERTs
- Security Sites
- Security Tools
- Antivirus Resources
- Security Apps for Smart Phones



Guidelines: Year 2014

- ▶ [Guideline on Safe BYOD Management](#)  **NEW**

Guidelines: Year 2013

- ▶ [Guideline on Implementing Cloud IAM](#) 
- ▶ [Guideline on Securing Public and Private Wi-Fi Networks](#) 
- ▶ [Guideline on Securing Mac OS X Mountain Lion](#) 
- ▶ [Updated Guideline on Mobile Devices Security](#) 
- ▶ [Guideline on Public Key Infrastructure \(PKI\)](#) 

Guidelines: Year 2012

- ▶ [Technical Guideline on Public Internet Access Points \(Computer Clubs, Cyber-Caravans and Post-Offices\)](#) 
- ▶ [Guideline on Strong Passwords and Passphrase](#) 
- ▶ [Guideline on Spam Control](#) 
- ▶ [Guideline on Auditing and Log Management](#) 
- ▶ [Guideline on Email Best Practices](#) 
- ▶ [Guideline on Debit or Credit Cards Usage](#) 
- ▶ [Guideline on Wireless Security](#) 
- ▶ [Guideline on Incident Handling and Reporting](#) 
- ▶ [Guideline on Windows 7 Parental Controls](#) 

Guidelines: Year 2011



Strategic Policies

- National Cyber Security Strategy
- Child Online Protection Action Plan
- Anti Spam Action Plan
- Critical Information Infrastructure Protection



Contact CERT-MU

- Hotline: 800-2378
- Website: www.cert-mu.org.mu
- General Queries: contact@cert-mu.gov.mu
- Incident Reporting: incident@cert-mu.gov.mu
- Mailing List Subscription: subscribe@cert-mu.gov.mu
- Vulnerability Reporting: vulnerability@cert-mu.gov.mu