Vulnerability Management Process
For
Government Data Center

Prepared by

Bhutan Computer Incident Response Team,
Department of IT & Telecom,
Ministry of Information & Communications

15 July, 2017

Table of Content

1. Overview

With countless cyber attacks perpetuated throughout the global IT infrastructure, it has changed the landscape of cyber world. Even the most sophisticated measures are proving to be challenging in keeping these threats at bay. With every new vulnerabilities discovered on count of thousands, the system owners are reminded of how unsafe their infrastructure are. There is no foolproof security compliances that has the capacity to assure 100 percentile security. However, it does not conclusively indicate that security could be neglected. As cyber security gains more attention of the IT industry, investors are showing interest to focus on security measures to counter cyber threats.

As BtCIRT's mandate, the team is working closely with its constituents to provide assistance in addressing security challenges through adoption of best practices, issuance of advisories, creating awareness, engaging media to disseminate information, to name a few. With most of the sensitive applications being hosted in the Government Data Center (GDC), the BtCIRT has prioritised its efforts to focus on this critical facility. This document is, therefore, produced as part of such initiative in conjunction with the risk assessment of the GDC carried out by the team.

This document is intended to provide high level overview of the vulnerability management workflow for Government Data Centre(GDC). It is aimed to provide reference to all GDC stakeholders to help understand the standards and procedures that are important in managing vulnerability. This document describes the process to be followed in assessing systems for vulnerability and adopt remedial methods based on the severity of the issue and criticality of the system. This documents assumes that regular backup of all systems are maintained.

For the purpose of protection of confidentiality of sensitive information gathered from GDC, redistribution of this document or sharing of information in part without the consent of the team is strictly restricted.

2. Roles and responsibilities

This section clearly defines the roles and responsibilities of BtCIRT and GDC team. The roles and responsibilities will define the expectations of each team. Within the GDC team, the responsibilities could be properly segregated. GDC administrator may further delegate the vulnerability patching jobs to the respective service owners.

2.1. BtCIRT

The team is assigned following roles:

a. Conduct vulnerability assessments of systems in GDC.
b. Provide vulnerability assessment reports to GDC.
c. Assist GDC in adopting recommendations when necessary.
d. Support during the change management.
e. Evaluate security requirements of any new systems prior to hosting in GDC.

f. Recommend international standards and best practices to enhance GDC infrastructure security.

2.2. Government Data Center

a. Acknowledge receipt of vulnerability assessment report and follow through the recommendations therein.
b. Register all the vulnerabilities in the Vulnerability register.
c. Determine whether the identified vulnerabilities are mitigable or accept the risks posed by the vulnerabilities.
d. Define and provide comprehensive plan to implement remediation measures recommended in vulnerability report in the timeframe defined under the Risk Mitigation section.
e. Monitor the performance of the network during the scanning process.
f. Share completion reports to BtCIRT when all identified issues are addressed successfully.
g. Maintain a vulnerability register.

3. Processes

3.1. Preparation

While unauthenticated scan shall be performed regularly, authenticated scans will be conducted quarterly. IP addresses range will be provided by GDC including the changed IP addresses. The planned date column in the table below indicates how authenticated scans are scheduled. The systems could be planned by the GDC team.

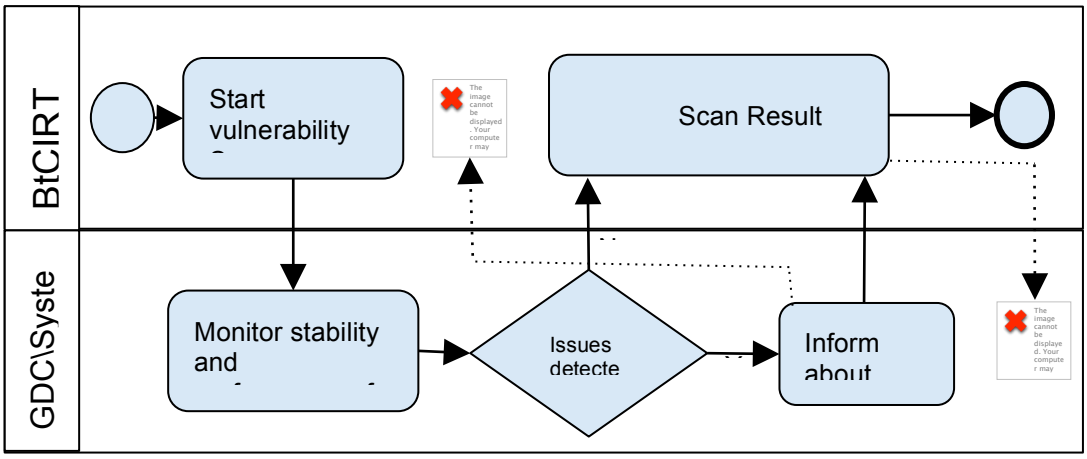
IP range	System Owner/Application Owner	Planned date	Contact
103.78.116.0/24	GDC/ <Agency Name>	October, 2017	+975-02-338606
103.78.117.0/24	GDC/ <Agency Name>/	January, 2018	+975-02-338606
103.78.111.0/24	GDC/ <Agency Name>	April, 2018	+975-02-338606
	GDC/ <Agency Name>	July, 2018	+975-02-338606

3.2. Vulnerability Scan

The vulnerability scan will be carried out during the planned dates and based on the new feeds received. Due to traffic generated by the scanning job, spike in the network usage is

expected. GDC team shall monitor the network performance during the scanning process and provide solutions if it severely affects the network. In the event of huge spike that can potentially disrupt the network, the team may request BtCIRT to suspend the job. Alternatively, the dates can be rescheduled for vulnerability scanning.

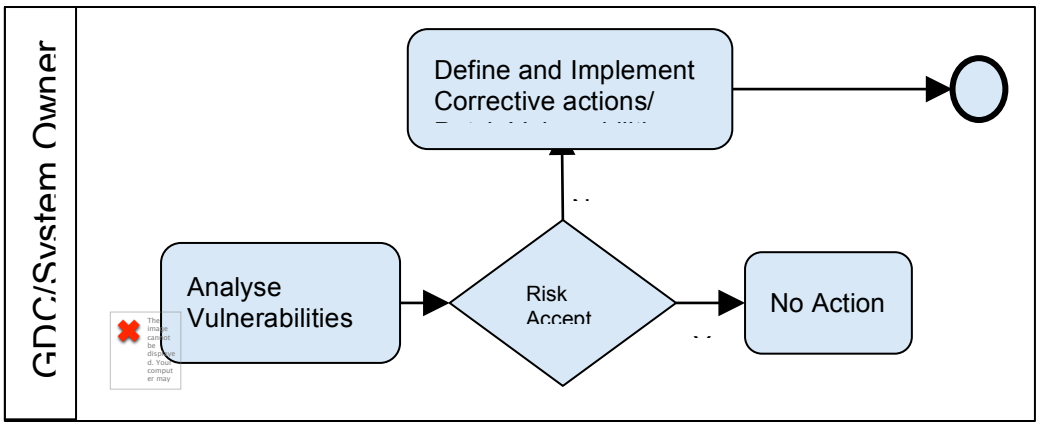
As depicted in the diagram below, the BtCIRT will initiate vulnerability scans on the network made accessible by GDC. The GDC team will confirm the vulnerabilities detected through manual check. False positives may be dropped with proper records. Any issue which occur during the scans, for example systems becoming unavailable or poor application response, should be recorded for future reference. In such cases, alternative actions may be defined to reduce the impact of future scans on the stability or performance of the target systems.



3.3. Define and Implement remediation

BtCIRT will provide vulnerability report with CVSS labelling. GDC/System Owner shall analyze the vulnerabilities, determine the associated risk levels based on asset value. The team shall plan to address_possible results of the proposed remediation before its deployment. The plan must include provision for server restoration, should any mishap occurs during the remediation process. Additionally, the team may also explore if any other measures are available to further reinforce configurations. It is recommended that a fresh backup is maintained before initiating the patching work.

The respective system owners will be required to evaluate risks associated with the vulnerabilities based on asset management. It is recommended that deadline for implementation remediation actions is set in accordance of priorities based on the level of risks. A form/ registration template is provided to assist the GDC team in managing vulnerabilities. The GDC team may choose to take no action if the risk are determined to have very low impact.



4. Risk Mitigation

Given the number of applications hosted at GDC, it would be very challenging for the GDC team to carry out corrective actions in one go. Instead, applications could be prioritised and managed based on criticality and value of the data stored by these applications and value of services provided by applications to the end users. It is advised that the GDC team should carry out this exercise for segregation or prioritisation. Asset value could indicate both the significance of the data as well as the physical asset of these systems.

Upon calculation of the risk value, the final classification of risk levels and prioritization of the corrective actions could be made in accordance with the following tables:

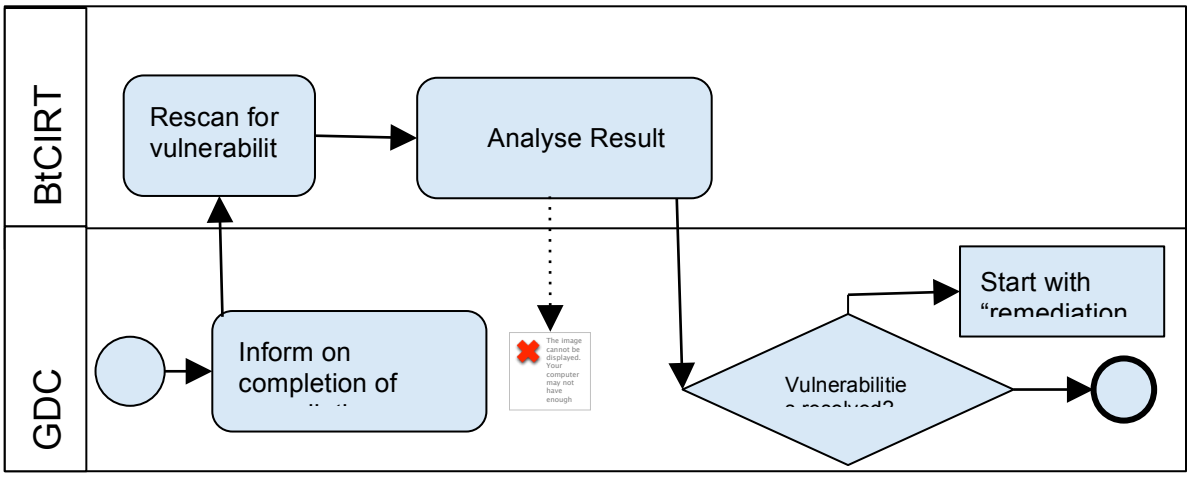
Severity \ Importance	Very important	Important	Normal
Critical	critical	medium	medium
High	High	medium	low
Medium	medium	low	low
Low	low	low	low

Priority level	Start	Response	Resolve
Critical	15 business minutes	20 business minutes	4 working days
Medium	1 business hour	2 business hours	7 working days
Low	6 business hours	1 working day	10 working days

The following table provides a template for registration of the vulnerabilities. The table will help record the vulnerabilities detected and action taken against it.

IP	Scan Date	Vulnerability Detected	Risk Rating/Priority	Corrective Action	Implementation date

5. Rescan



Once the GDC/System Owner completes remediation actions, BtCIRT will rescan the systems to confirm the vulnerabilities are resolved and check for any residual risk. If issues continue to persist, then the team to work on some other remediation actions.