rebit.org.in

रिज़र्व बैंक सूचना प्रौद्योगिकी प्राइवेट लिमिटेड
Reserve Bank Information Technology Pvt. Ltd.

ReBIT, 18th Floor,
CyberOne Business Park Sector 30A,
Vashi, Navi Mumbai 400703

info@rebit.org.in

# Research Note on Vulnerability Disclosure

## Scoping global scenario of vulnerability disclosure policies/laws

Date: May, 2018
Author: Ranjeet Rane

Abstract:
This whitepaper discusses the different models of vulnerability disclosures presently in practice. Several case studies from different geographies, providing brief synopsis of how different countries have shaped or are in the process of shaping their responsible/coordinated vulnerability disclosure policies are discussed.

# Table of Contents

# Responsible Vulnerability Disclosure [RVD]

## Definition

In computer security or elsewhere, responsible disclosure is a vulnerability disclosure model in which a vulnerability or issue is disclosed selectively to exposed party/parties and made public only after a period of time allowing the vulnerability or issue to be patched or mended. This period distinguishes the model from full disclosure [1]. This process is also referred to as ‘Coordinated Vulnerability Disclosure’ [CVD] in some countries.

## Introduction

Software and software-based products have vulnerabilities. Left unaddressed, these vulnerabilities pose a risk to the systems on which they are deployed as well as the people who depend on them. In order for vulnerable systems to be fixed, those vulnerabilities must first be found. Once found, they must be patched or configurations must be modified accordingly. Collaboration between technology service providers and security researchers is an important part of information security best practices. Security researchers [as well as customers, academics, journalists, and tech hobbyists] often discover vulnerabilities and organizations, both public and private, can benefit from having in place a mechanism for disclosing them and a process to work with such disclosures. Timely intervention can not only prevent technical losses but also help in averting reputational crisis.

# Types of Disclosures

RVD/CVD programs are mistakenly referred to as bug-bounty programs that came into being after the Bugtraq vulnerability mailing list became popular in the early ‘80s. [2] However, vulnerability disclosure practices go beyond bug bounty programs and are usually classified into four categories.

## Non-Disclosure:

A non-disclosure practice is the one where an individual or organization keeps the vulnerability information to itself with the intention to keep the information out of public domain. Some vendors and security firms promote a policy of nondisclosure. The general understanding is that that the vulnerability information can be controlled and only “trusted” individuals need to be informed. This is aimed at ensuring that they can “protect” the vulnerable systems until a fix can be made available.

## Full Disclosure:

Full disclosure essentially means to disseminate maximum information about system vulnerabilities and attack tools so that potential victims are as knowledgeable as attackers. Full disclosure is expected to keep technology vendors motivated towards providing timely patches/fixes to the disclosed vulnerability. Failure in doing so may result in negative publicity that may have revenue and reputational costs.

## Limited Disclosure:

This practice is an extension of non-disclosure, wherein, during the initial phases of disclosure only a small group is allowed access to the complete details of the vulnerability. This group usually consists of the discloser, the vendor and a third party coordinator if necessary. The public disclosure, if any, only describes the flawed product and includes very few details about the vulnerability.

## Responsible Disclosure:

This is a multi-stage process involving multiple stakeholders. It begins with the discovery of a vulnerability and the availability of right channels to report it. Legal immunity from prosecution is one of the primary expectations of the researchers responsibly reporting a vulnerability. It continues through phases of initial contact with coordinating agency, continued communication with vendor/resource owner, patch release, public disclosure and finally release of details of the exploit. Different countries are trying this approach, some of the important ones are discussed in this document.

# Global Case Studies

## Netherlands

The National Cyber Security Centrum [National Cyber Security Center, NCSC] of Netherlands has put in place a Responsible Disclosure Policy that aims to contribute to the security of ICT systems and control the vulnerabilities in them by reporting those vulnerabilities in a responsible manner and acting on the reports appropriately so as to prevent or limit potential damages to the maximum possible extent. The NCSC is not the point of contact for the disclosure, however it acts as a coordination agency if it is approached with a disclosure. The Netherlands program is among the most mature VD programs and a benchmark for such policies across Europe.

## Australia

CERT Australia has put in place a VD policy that outlines how it will coordinate the disclosure of information relating to reported vulnerabilities that are not publicly known. This disclosure will also provide vendors and developers with additional time to mitigate the vulnerabilities and enable affected systems of national interest to reduce their exposure. There is an implicit agreement to operate in accordance with the relevant local law of their jurisdiction and the CERT will not recommend or pursue legal action on behalf of another party. They also do not engage in giving rewards or incentives, however the vendor or technology resource owner may opt to do so.

## European Union:

The European Union Agency for Network and Information Security [ENISA] is the nodal agency for responsible vulnerability disclosures. However, only three of 28 member states currently have a policy on responsible disclosure, and 13 are in various stages of developing one. To remedy the situation, a task force appointed last year has recommended that vulnerability disclosure policy to be harmonized across the EU on the basis of two International Standards Organization (ISO) standards: ISO 30111 on vulnerability handling and ISO 29147 on vulnerability disclosure. The EU Cybersecurity Act, that will be presented before the EU Parliament later in March 2018 is expected to provide cybersecurity researchers in the European Union legal certainty and consistent standards across its 28 member states.

## Unites States of America

The USA has attained high levels of maturity in their vulnerability disclosure practices. They drive it as a mix of events [3] and a Vulnerability Disclosure Policy that is coordinated by the ICS-CERT, the agency that works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community.

The USA passed the Cyber Vulnerability Disclosure Reporting Act early this year. It directs the Secretary of the U.S. Department of Homeland Security (DHS) to prepare a report describing the policies and procedures to coordinate cyber vulnerability disclosures. Under the Homeland Security Act of 2002 and the Cybersecurity Information Sharing Act of 2015 (CISA), DHS is responsible for working with industry to develop DHS policies and procedures for coordinating the disclosure of cyber vulnerabilities.

In accordance with provisions the of National Security Policy Directive-54/Homeland Security Policy Directive-23, Cybersecurity Policy, and the Joint Plan for the Coordination and Application of Offensive Capabilities to Defend U.S. Information Systems, they have also rolled out a Vulnerabilities Equities Policy [VEP] and Process for departments and agencies of the United States Government in November 2017. The VEP decides whether to disseminate vulnerability information to the vendor/supplier in the expectation that it will be patched, or to temporarily restrict the knowledge of the vulnerability to the United States government, and potentially other partners, so that it can be used for national security and law enforcement purposes, such as intelligence collection, military operations, and/or counterintelligence. The most recent development in the USA is the 'Protecting Our Ability to Counter Hacking' Act of 2017 or the PATCH Act, which is presently under consideration of the US Congress. If it becomes a law, it will mandate the VEP to disclose information in public domain.

# Indian Scenario

The National Critical Information Infrastructure Protection Centre (NCIIPC) was created by the Government of India with a mission “To take all necessary measures to facilitate protection of Critical Information Infrastructure, from unauthorized access, modification, use, disclosure, disruption, incapacitation or distraction through coherent coordination, synergy and raising information security awareness among all stakeholders.” [4]

The NCIIPC website has a pdf form for reporting vulnerabilities, which is directed more towards vendors and not at researchers or general public. The process isn’t backed by any documented policy or amendments in relevant laws that would grant immunity in case of a genuine disclosure. The CERT-In is a member of the Forum of Incident Response and Security Teams [FIRST] but it doesn’t have a vulnerability disclosure policy outlined yet. A document titled “Information Security Policy for Protection of Critical Information Infrastructure” [5] dating to May 2006, mandates that critical information infrastructure should be protected against wrongful disclosure by CERT-In.

Private players like Paytm [6] have come up with their own vulnerability disclosure policies. However these are more similar to ‘bug bounty’ programs do not have legal backing and are subject to terms and conditions defined by the private organization only.

# References

1. **Responsible Disclosure** – Wikipedia https://en.wikipedia.org/wiki/Responsible_disclosure [last accessed March 2018]
2. **Vulnerability Disclosure, Stephen Shepard**, SANS InfoSec Reading Room - https://www.sans.org/reading-room/whitepapers/threats/define-responsible-disclosure-932 [last accessed March 2018]
3. **Hack The Pentagon - A Department of Defense Vulnerability Program** - https://www.hackerone.com/resources/hack-the-pentagon [last accessed March 2018]
4. **About Us, National Critical Information Infrastructure Protection Centre** - http://nciipc.gov.in/ [last accessed March 2018]
5. **Information Security Policy for Protection of Critical Information Infrastructure, 2006** - http://mapit.gov.in/securityaudit/downloads/CERT-In%20Info_Sec_Policy.pdf [last accessed March 2018]
6. **Paytm Bug Bounty Program** - https://bugbounty.paytm.com/ [last accessed March 2018]

# Bibliography

**Forum of Incident Response and Security Teams [FIRST]**
https://first.org/members/teams/
**Blog of Josip Franjković**, security researcher and Facebook's top Whitehat reporters since 2013 - https://www.josipfranjkovic.com/
**Known private bug bounty programs** -
https://en.wikipedia.org/wiki/Bug_bounty_program
**Common Vulnerabilities and Exposures** (CVE®) -
https://cve.mitre.org/about/index.html
**A Framework for a Vulnerability Disclosure Program for Online Systems** [Computer Crime & Intellectual Property Section Criminal Division, U.S. Department of Justice] - https://www.justice.gov/criminal-ccips/page/file/983996/download
**Vulnerabilities Equities Policy and Process for the United States Government** [Nov, 2017] -
https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF