1. Background

Patching is a critical task in IT infrastructure maintenance. New security vulnerabilities get released every day.In practise, at our client, software patches are applied manually, in an adhoc manner. When there are hundreds of patches available for system assets, it becomes crucial to know the priority of patches. Many times the priority decision is not obvious to make. There are several approaches possible. Two most common and important criteria used in deciding the order of applying different patches are:

1. How important the host machine is, probably a function of:

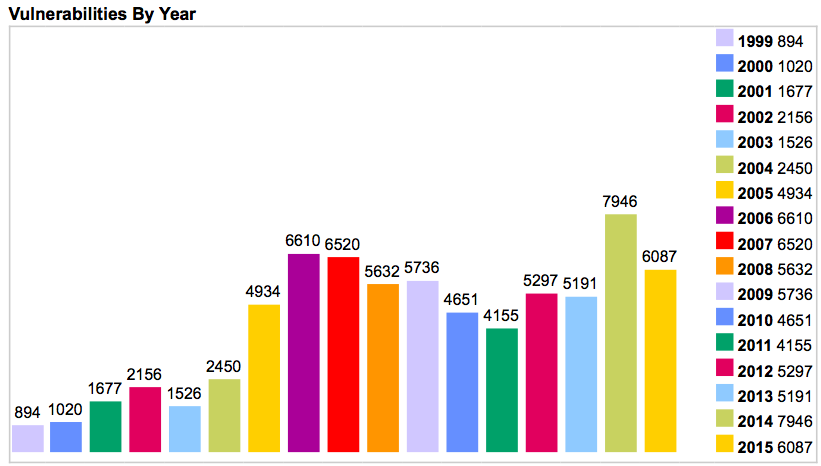
(a) its placement in network (e.g. internal or external server)

(b) the importance of services being run on it

(c) availability of backups (load balancing)

2. How severe is the vulnerability for which patch needs to be applied

2. Motivation

 Reference: http://www.cvedetails.com/browse-by-date.php

Vulnerabilities are getting increased year after year. Therefore the need for prioritising patches are also increasing.In order to prioritise the patches, we need to assess the severity of the patches. Common Vulnerabilities and Exposures (CVE) provides a CVSS score from 1 to 10 for all the vulnerabilities and this is accepted as a standard mechanism to assess the severity of the vulnerabilities by a wide range of organisations and companies.

However, the CVSS Score is not sufficient to prioritize the patches since we also have to take into account the importance of host machine on which patch will be applied. Eg: A patch for a software used in a front end server will not have the same priority as a patch for a software that is used in an internal tool.This importance is denoted as the environmental impact in this report.

The motivation of this project is to prioritize the patches by combining the CVSS Score as well as the environmental impact.