Example of CVSS based Patching Policy

1.0 Overview:

1. This policy has been put in place to establish a mechanism for identifying and ranking security vulnerabilities across all teams within the Security Alerts Team .

2.0 Purpose:

The purpose of this policy is to provide a framework for vulnerability identification, threat assessment, priority ranking and voluntary or involuntary remediation via patch distribution by manual or automated methods.

3.0 Scope:

3.1 The general scope of this policy applies to all CompanyX assets managed by members of the Security Alerts Team that contain software subject to security alerts.

3.2 Each group adopting this policy will specify management representatives for their team during the bi-weekly Security Alerts Team meeting. Updates including attendance, alerts discussed, and actions recommended will be mailed to the responsible mangers via the <satt-managers@xxx.com> email alias.

4.0 Responsibilities:

4.1 The Security Alerts Team , composed of Infosec and operational team members periodically identifies significant security vulnerabilities that may impact CompanyX assets. This team will also make recommendations about the timeline for patch installation based on the threat.

4.2 The Security Alerts Team will continue to monitor the status of each alert discussed, being sure to track any changes in the status of the alert (I.E. exploit availability, patch availability, etc.) and update the temporal score of CVSS to reflect these changes. These changes could raise or lower the initial CVSS score. Any updates to an alert will be tracked by the InfoSec SATT duty representative.

4.3 The patch or update will be automatically or manually applied to each host depending on the priority ranking assigned to each patch as outlined in the section 5.0. Responsibility for patch quality assurance, patch distribution, audit, and adding the patches to the standard image is determined by each support organization.

5.0 Priority Ranking:

5.1 All updates will be ranked as P1-P4

5.2 Priority ranking depends on the CVSS score of a vulnerability. The CVSS score is determined based on access conditions and impact of a vulnerability, as well as time dependant qualities of a vulnerability, such as patch and exploit availability.   The Security Alerts Team POC is responsible for assigning a CVSS score to an alert. The vulnerability is then scored in the alerts database and discussed during the scheduled Security Alerts Team meeting.

5.3 A priority ranking will be given to an alert based on the CVSS score. Any borderline alerts will be moved up or down based on the consensus of the Security Alerts Team members. The alerts priority will be assigned based on the following chart:

CVSS Vulnerability Assessment Results:

CVSS Score	Priority	Patch SLA
0	P4	Discretionary
.1-3	P3	Next Patch Cycle (3-6 months)
4-6	P2	4 Weeks Max
7-10	P1	2 Weeks Max

6.0 Enforcement:

6.1 Criteria for Enforcement are dependent on the Priority Ranking of a patch. Enforcement can include:

- Automated application of a patch or operational change to the system
- Black Holing of the system to remove it from the network until the patch is applied
- Power deactivation of the system
- Removal of the system from the data center
- Re-installation of the OS based the IT supported standard image (I.E. WINES, CompanyX Linux, Jumpstart, etc).

7.0 Exceptions:

7.1 No scoring system is flawless and will never replace common sense. Each hosting group reserves the right to individually lower or raise a priority ranking for individual servers or a group of servers based on business impact. Priority adjustments need to be signed off by a management representative responsible for the Asset in question.

7.2 A written explanation of any priority adjustment must be submitted to the Security Alerts Team <security-alerts-team@companyX.com>.

7.3 At any time an alert may be created or escalated to P1 status regardless of the CVSS score if there is a credible risk to CompanyX.

8.0 References

8.1 CVSS FAQ:

9.0 Approval:

The following individuals have agreed to the content and scope of this contract:

Author Michael Scheck mscheck@cisco.com