



Vulnerability Management Baseline Standards

Rationale

The campus maintains that the level of security controls that should be implemented on a server should be relative and proportionate to the level of risk of unauthorized access for that the server. This level of risk may be attributed to multiple factors such as network topology, services and resources offered, and type of information managed¹. The campus has devised a three tier server risk category system (high, medium and low risk) to assist server owners and technical staff in implementing the level of protection required by their servers. The characteristics of servers belonging to each tier are given in the below table.

Server Risk Categories

Server Risk Category	HIGH	MEDIUM	LOW
Description of Server Characteristics	1) Contain Protected Level 1 Information and/or 2) Provide enterprise wide services and/or 3) Have high availability requirements	1) Contain Protected Level 2 or 3 Information and/or 2) Provide administrative services and/or 3) Have medium or varied availability requirements.	1) Contain no Protected Level Information and/or 2) Have low availability requirements

The Foundstone Vulnerability Management Tool

McAfee Foundstone is a vulnerability management solution that helps system administrators determine how emerging threats affect the risk profile of their servers. McAfee Foundstone provides an executive dashboard where a system administrator can view the security status of systems.

The Server Risk Report

The Information Security Office has created the Server Risk Report to provide information for technical staff and server owners about the security posture of campus servers for which they are responsible. The report utilizes data from both OMNI and McAfee Foundstone, and uses an algorithm to calculate weighted risk scores for campus servers.

The higher the server risk score, the less time the system administrator has to remediate the vulnerabilities. This is because the overall risk to the campus network is higher, and therefore more immediate. System administrators can improve the risk score for servers in their charge by following the steps outlined in the Server Risk Report Preparation page².

To access the report, system administrators and server owners can visit: <https://insight.csuchico.edu> (the report is best viewed using Internet Explorer). Once signed in, click on the “Information Security” folder.

¹ The levels of protected information are defined in the “Data Classification and Protection Standard” at <http://www.csuchico.edu/ires/security/documents/DataClassificationStandard3.26.pdf>

² The Server Risk Report Preparation can be found at <https://wiki.csuchico.edu/confluence/display/isec/Server+Risk+Report+Preparation>



New Servers

Before being connected to the campus network, all new servers should be scanned with a McAfee Foundstone credentialed scan. All discovered vulnerabilities should be remediated, and the server should then be rescanned using a credentialed scan.

Servers with residual high and/or medium level vulnerabilities, which do not have written exemptions from an appropriate administrator, should not be connected to the campus network until those vulnerabilities are remediated.

Existing Servers

All existing servers should be scanned (using credentialed scans) according to the Server Risk Category to which they belong:

- High Risk Category Servers should be credential scanned at least once a week
- Medium Risk Category Servers should be credential scanned at least once every two weeks
- Low Risk Category Servers should be credential scanned at least once every four weeks

Vulnerabilities discovered during scans should be remediated prior to the next scheduled scan, and vulnerabilities that cannot be remediated should have written exception from an appropriate administrator (e.g., department chair, director, dean, etc.).

The below table outlines the remediation time limits for vulnerabilities that do not have written exceptions. The time limits are based on a combination of the:

- Server Risk Report Score (Red, Yellow or Green)
- Server Risk Category (High, Medium or Low)
- McAfee Foundstone Vulnerability Risk Classification (High, Medium or Low)

These three factors are used together to give system administrators realistic standards for vulnerability remediation, based on the total risk to the server system and campus network.



Server Risk Report Score	RED	YELLOW	GREEN
High Server Risk Category Systems			
High Foundstone Vulnerability Score	1 Day	3 Days	1 Week
Medium Foundstone Vulnerability Score	3 Days	1 Week	2 Weeks
Low Foundstone Vulnerability Score	2 Weeks	3 Weeks	4 Weeks
Medium Server Risk Category Systems			
High Foundstone Vulnerability Score	3 Days	1 Week	2 Weeks
Medium Foundstone Vulnerability Score	1 Week	2 Weeks	4 Weeks
Low Foundstone Vulnerability Score	2 Weeks	4 Weeks	6 Weeks
Low Server Risk Category Systems			
High Foundstone Vulnerability Score	1 Week	2 Weeks	4 Weeks
Medium Foundstone Vulnerability Score	2 Weeks	4 Weeks	8 Weeks
Low Foundstone Vulnerability Score	3 Weeks	6 Weeks	10 Weeks



Review/Approval History

Date	Audience	Action	Version
1/29/2009	System Security Meeting	Presented	v1.0
1/30/2009	CIO	Approved	v1.0
2/2/2009	Cabinet	Reviewed	v1.0
3/2/2009	Cabinet	Approved	v1.0