INFORMATION SECURITY GUIDELINE

Severity Ratings for Vulnerabilities (CVSS v2.0)

Introduction

1. The purpose of this guideline is to summarize the standardized ratings, in the latest version of the Common Vulnerability Scoring System, which was issued by the Forum of Incident Response and Security Teams (FIRST) and the Common Vulnerability Scoring System-Special Interest Group (CVSS-SIG). These ratings are used by UBC in determining priorities for resolving vulnerabilities and applying patches.
2. This guideline has been issued by the Chief Information Officer to supplement the Reporting Information Security Incidents standard. Compliance with this guideline is recommended, but not mandatory. Questions about this guideline may be referred to information.security@ubc.ca.

CVSS Severity Ratings

Rating	Description	Examples
High (CVSS 7.0 – 10.0)	Risks a total to partial system compromise by either DoS or arbitrary code execution with privileges being potentially escalated to the administrator/root level. Could interfere with important services/daemons that are only recoverable by the root/Administrator account, provide full read permissions to the file system, provide administrative backdoors or could cause the host to perform unwanted actions.	Rootkits, spam botnet installation, default passwords, DoS, kernel-level crash such as a Red or Blue Screen of Death, service-level crashes, Trojan/worm installation, viruses, user-space software crashes, system command injection, remote code execution, heap/stack/buffer overflow or underflow attacks that compromise an administrator account or an unprivileged user account.
Medium (CVSS 4.0 – 6.9)	Risks fraud or participation in attacks of other hosts. Code execution may be involved, but it is not permanently installed or requires user involvement to execute each time. Disclosure of security mechanisms, and therefore weaknesses, may be involved.	Cross-site scripting (XSS), open mail relays, spoofing, list of security settings.
Low (0.1 – 3.9)	Risks temporary service instability or malfunction with no possibility of privilege escalation or code execution.	Missing non-security patches or hotfixes.

Related Documents

Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems

Vulnerability Management standard