Nanyang Technological University

AY2021-2022 Semester 2

CE/CZ4067 SOFTWARE SECURITY

Tutorial 2: Risk Analysis with CVSS

1. The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities [1]. CVSS consists of three metric groups: Base, Temporal, and Environmental. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score. Thus, CVSS is well suited as a standard measurement system for industries, organizations, and governments that need accurate and consistent vulnerability severity scores. Two common uses of CVSS are calculating the severity of vulnerabilities discovered on one's systems and as a factor in prioritization of vulnerability remediation activities. The National Vulnerability Database (NVD) provides CVSS scores for almost all known vulnerabilities. The NVD supports both CVSS v2.0 and v3.X standards.

   (a) Read the user guides for CVSS v2.0 (https://www.first.org/cvss/v2/guide). What are the purposes of introducing the temporal and environmental metrics?

   (b) Read the user guides for CVSS v3.1 (https://www.first.org/cvss/v3.1/user-guide). Discuss the main differences between v2.0 and v3.1, and the rationales of introducing the new changes.

2. Find information about the vulnerability CVE-2013-1937 online.

   (a) A CVSS 3.X vector string "AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N" is assigned. Calculate a base score using the CVSS 3.1 calculator (https://www.first.org/cvss/calculator/3.1). Explain the rationale behind each metric value. For example, why is "Changed" chosen for "Scope"?

   (b) For some purposes, it is useful to have a textual representation of the numeric scores. All CVSS scores can be mapped to the qualitative ratings defined in Table 1. What is the qualitative severity rating of the vulnerability? Do you think the rating is reasonable? Why?

Table 1: Qualitative severity rating scale.

Rating	CVSS Score
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

References

[1] NVD - vulnerability metrics. https://nvd.nist.gov/vuln-metrics/cvss, November 2021.