10.5 Vulnerabilities

It is very important to precisely understand what a vulnerability is. A vulnerability is a flaw in a system that an attacker could exploit to attack the system.

10.5.1 CVE

The most common list of vulnerabilities is the CVE list. Common Vulnerabilities and Exposures (CVE) is a list maintained by the Mitre Corporation at https://cve.mitre.org/. It is not only the most common, but also the most comprehensive vulnerability list. The CVE list was designed to provide a common name and description for a vulnerability. This allows security professionals to effectively communicate about vulnerabilities. In the past, CVEs had been designated by a CVE ID in the format of CVE-YYYY-NNNN. This format only allows 9,999 unique identifiers per year. The new format is CVE prefix + Year + Arbitrary Digits and allows any number of digits.

10.5.2 NIST

The U.S. National Institute of Standards and Technology maintains a database of vulnerabilities that you can access at https://nvd.nist.gov/.

NIST also uses the CVE format. For example, CVE-2017-12371 is described as “A ‘Cisco WebEx Network Recording Player Remote Code Execution Vulnerability’ exists in Cisco WebEx Network Recording Player for Advanced Recording Format (ARF) and WebEx Recording Format (WRF) files. A remote attacker could exploit this by providing a user with a malicious ARF or WRF file via email or URL, convincing the user to launch the file. Exploitation of this could cause an affected player to crash and, in some cases, allow arbitrary code execution on the system of a targeted user.”

10.5.3 OWASP

The Open Web Application Security Project is the standard for web application security. OWASP has published a number of important documents. For our current purposes, the most important is their top 10 list, located at https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.

Every several years a new 10 web application vulnerabilities list is published. This list contains the actual vulnerabilities most frequently found in web applications.