Оценка уровня угрозы уязвимости

Методом ранжирования угроз

Общая Система Оценки Уязвимости

(CommonVulnerabilityScoringSystem, CVSS)

- Данная система предназначена для классификации уязвимостей по **шкале критичности** от 0 до 10:
  - **0,0 – 3,9 — низкая степень;**
  - **4,0 – 6,9 — средняя степень;**
  - **7,0 – 9,9 — высокая степень;**
  - **10 — критическая степень.**
- Оценка (отнесение к уровню критичности) уязвимости производится на основе набора показателей:
- ***1).вектор доступа, 2).сложность доступа, 3). аутентификация, 4).влияние на конфиденциальность, 5). влияние на целостность, 6).влияние на доступность***.

Вектор доступа

- Вектор доступа (AccessVector) определяет, как уязвимость может быть обнаружена и использована.
  - **Local – злоумышленнику необходим физический доступ к компьютеру;**
  - **Adjacent Network – злоумышленнику необходим доступ к локальной сети;**
  - **Network – уязвимость может быть использована из сети Интернет.**

Сложность доступа

- Сложность доступа (AccessComplexity) определяет, насколько сложно провести атаку на систему через уязвимость после получения доступа к ней.
  - **High – злоумышленнику необходимо иметь высокую квалификацию, использовать нестандартные пути реализации атаки и обладать значительной информацией о системе. Конфигурация ПО является достаточно экзотической;**
  - **Medium – злоумышленник должен иметь ограниченные права в системе. Конфигурация ПО отличается от конфигурации по умолчанию;**
  - **Low – конфигурация по умолчанию. Круг тех, кто может являться злоумышленником, не ограничен.**

Аутентификация

- Аутентификация (Authentification) определяет, сколько уровней аутентификации и авторизации должен пройти злоумышленник, прежде чем он получит возможность использовать уязвимость в системе.
  - **Multiple – множественная аутентификация и авторизация;**
  - **Single – однократная авторизация;**
  - **None – отсутствие аутентификации и авторизации.**

Влияние на конфиденциальность

- Влияние на конфиденциальность (ConfidentialityImpact) определяет влияние успешной атаки с использованием уязвимости на конфиденциальность системы и данных.
  - **None – отсутствие влияния;**
  - **Partial – злоумышленник получает доступ к ограниченному набору данных;**
  - **Complete – злоумышленник получает полный доступ ко всем данным.**

Влияние на целостность

- Влияние на целостность (IntegrityImpact) определяет влияние успешной атаки с использованием уязвимости на целостность данных и системы.
  - **None – отсутствие влияния;**
  - **Partial – частичная потеря целостности (возможна модификация части конфигурации системы, часть данных может быть подменена и пр.);**
  - **Complete – возможна подмена любых данных, модификация конфигурации и процессов всей системы.**

Влияние на доступность

- Влияние на доступность (AvailabilityImpact) определяет влияние успешной атаки с использованием уязвимости на доступность системы.
  - **None – отсутствие влияния;**
  - **Partial – частичная недоступность (падение производительности системы или ее частей, непродолжительные перерывы в доступности данных);**
  - **Complete – полная недоступность системы, отказ в обслуживании.**