УДК 004.056.5

Бубакри Камель, магистрант, Полякова Н.П., доц. к.т.н. – научный руководитель

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СИСТЕМ ОЦЕНКИ УЯЗВИМОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

Запорожская государственная инженерная академия, кафедра ПЗАС

В настоящее время IT-персонал вынужден выявлять уязвимости различных программных и аппаратных платформ. Существует необходимость расставить приоритеты для всех этих уязвимостей, чтобы в первую очередь исправлять те из них, которые представляют наибольшую опасность. Уязвимостей, подлежащих устранению много, и они оцениваются по разным шкалам существующих систем оценки уязвимостей, которые созданы коммерческими и некоммерческими организациями. Каждая из этих систем имеет свои преимущества, отличаются же они по тому, какой признак измеряется. Например, система CERT/CC использует значения оценок от 0 до 180 и учитывает такие факторы, как например, подвержена ли Интернет-инфраструктура риску и какой тип предусловий нужен для эксплуатации уязвимости. Система анализа уязвимостей SANS учитывает, в какой конфигурации найдена уязвимость – стандартной или нет, является ли система клиентом или сервером. Система оценки от Microsoft пытается отразить сложность эксплуатации и общее воздействие от эксплуатации уязвимости. Эти системы оценки являются полезными, но они представляют подход, при котором считается, что последствия эксплуатации уязвимости одинаковы для частного лица и для компании. CVSS является понятным, прозрачным и общепринятым способом оценки IT-уязвимостей для руководителей, производителей приложений и средств поддержания информационной безопасности, исследователей и др.

Общая система оценки уязвимостей (CVSS) или **Common Vulnerability Scoring System**, это открытая схема, которая позволяет обмениваться информацией об IT-уязвимостях. Система оценки CVSS состоит из 3 метрик: базовая метрика, временная метрика и контекстная метрика. Каждая метрика представляет собой число (оценку) в интервале от 0 до 10 и вектор – краткое текстовое описание со значениями, которые используются для вывода оценки. Базовые CVSS-метрики составляются для того, чтобы определить и отобразить основные характеристики уязвимости. Эта попытка объективно охарактеризовать уязвимость дает пользователям ясное и интуитивно понятное представление об уязвимости. Затем пользователи могут использовать временные и контекстные группы метрик, чтобы получить более подробную информацию об уязвимости с учетом своей среды. Такой подход позволяет принимать обоснованные решения при выборе способа минимизации риска от наличия уязвимости.

Использование CVSS предоставляет следующие выгоды:

- стандартизованная оценка уязвимостей;
- открытость системы;
- приоритезация рисков.

Группа базовых метрик CVSS представляет основные существенные характеристики уязвимости, которые не изменяются со временем и не зависят от среды. Она состоит из:

- Access Vector (AV) - Вектор доступа. Определяет эксплуатирована ли уязвимость с близи или с далека.
- Access Complexity (AC) - Сложность доступа. Отображает сложность эксплуатации атаки, если злоумышленник получил доступ к целевой системе.
- Authentication (Au) – Аутентификация. Отображает количество этапов аутентификации, которые злоумышленник должен пройти в целевой системе, чтобы эксплуатировать уязвимость.

- Confidentiality Impact (C) - Влияние на конфиденциальность. Отображает влияние успешной эксплуатации уязвимости на сохранение конфиденциальности в системе.
- Integrity Impact (I) - Влияние на целостность. Отображает влияние успешной эксплуатации уязвимости на целостность системы.
- Availability Impact (A) - Влияние на доступность. Отображает влияние успешной эксплуатации уязвимости на доступность информационных ресурсов системы.

Группа временных метрик представляет такие характеристики уязвимости, которые могут измениться со временем, но не зависят от среды:

- Exploitability (E) - Возможность использования. Отображает наличие или отсутствие кода или техники эксплуатации.
- Remediation Level (RL) - Уровень исправления. Предлагается для временного исправления уязвимости до того момента, когда будет выпущено официальное исправление или обновление.
- Report Confidence (RC) - Степень достоверности отчета. Отображает степень конфиденциальности информации о существовании уязвимости и достоверность известных технических деталей.

Группа контекстных метрик представляет такие характеристики уязвимости, которые зависят от среды:

- Collateral Damage Potential (CDP) - Вероятность нанесения косвенного ущерба. Отображает потенциальную возможность повреждения или утраты собственности или оборудования, а также может оценивать экономические потери, связанные с производительностью или доходом.
- Target Distribution (TD) - Плотность целей. Отображает процент уязвимых систем от всех имеющихся систем.
- Security Requirements (CR, IR, AR) - Требования к безопасности: Позволяют аналитику определить CVSS-оценку в зависимости от важности уязвимого устройства или программного обеспечения для организации, измеренной в терминах конфиденциальности, целостности и доступности.

Выводы:

1. Изучены алгоритмы вычисления оценок уязвимостей IT-продуктов.
2. Создан программный продукт, реализующий просчеты по изученным алгоритмам, который наглядно представляет результаты расчетов, а так же имеет множество других возможностей для удобного восприятия информации об уязвимости и принятия необходимых решений по их устранению.

Литература

1. Шнаймер Б. Секреты и ложь: Безопасность данных в цифровом мире: Питер, 2003. – 367с.
2. Отчет IBM Internet Security Systems X-Force® о состоянии информационной безопасности в 2007 г. Статистические тенденции
3. Малюк А. Информационная безопасность: Концептуальные и методологические основы защиты информации: Горячая линия – Телеком, 2004. – 280с.
4. Philip S. , Robert H. , Richard M. , Michael S. Finding and fixing Vulnerabilities in Information systems: The vulnerability assessment and mitigation methodology: RAND 2003. – 117c.