Классификация уязвимостей и атак

1. Основные понятия
2. Классификация уязвимостей
3. Классификаторы
4. Метрики
5. Классификация атак

Основные понятия

Угроза - это потенциально возможное событие, явление или процесс, которое посредством воздействия на компоненты информационной системы может привести к нанесению ущерба

Уязвимость - это любая характеристика или свойство информационной системы, использование которой нарушителем может привести к реализации угрозы.

Атака - это любое действие нарушителя, которое приводит к реализации угрозы путём использования уязвимостей информационной системы.

Источники возникновения уязвимостей

- Уязвимости закладываются на этапе проектирования
- Уязвимости возникают на этапе реализации (программирования).
- Уязвимости являются следствием ошибок, допущенных в процессе эксплуатации информационной системы.

Классификация уязвимостей по уровню в инфраструктуре АС

- К уровню сети относятся, например уязвимости сетевых протоколов - стека TCP/IP.
- Уровень операционной системы охватывает уязвимости конкретной ОС.
- На уровне баз данных находятся уязвимости конкретных СУБД.
- К уровню приложений относятся уязвимости программного обеспечения.

Классификация уязвимостей по степени риска

- **Высокий уровень риска**

  Уязвимости, позволяющие атакующему получить непосредственный доступ к узлу с правами администратора, или в обход межсетевых экранов, или иных средств защиты.

- **Средний уровень риска**

  Уязвимости, позволяющие атакующему получить информацию, которая с высокой степенью вероятности позволит получить доступ к узлу.

- **Низкий уровень риска**

  Уязвимости, позволяющие злоумышленнику осуществлять сбор критической информации о системе.

Примеры уязвимостей

(база данных компании ISS)

Название: nt - getadmin - present

Описание: проблема одной из функций ядра ОС Windows NT , позволяющая злоумышленнику получить привилегии администратора

Уровень: ОС

Степень риска: высокая

Источник возникновения: ошибки реализации

Название : ip-fragment-reassembly-dos

Описание: посылка большого числа одинаковых фрагментов IP - датаграммы приводит к недоступности узла на время атаки

Уровень: сеть

Степень риска: средняя

Источник возникновения: ошибки реализации

Классификаторы

- CVE
- BID
- OSVDB
- Secunia
- ISS X-Force

CVE

Common Vulnerabilities and Exposures (CVE) -

это список стандартных названий для общеизвестных уязвимостей.

Основное назначение CVE - это согласование различных баз данных уязвимостей и инструментов, использующих такие базы данных.

Например, одна и та же уязвимость может иметь различные названия в базе данных Internet Scanner и CyberCop Scanner .

Поддержку CVE осуществляет MITRE Corporation (www.mitre.org).

Процесс получения индекса CVE (CVE entry) начинается с обнаружения уязвимости.

Затем уязвимости присваивается статус кандидата CVE и соответствующий номер (CVE candidate number).

После этого происходит обсуждение кандидатуры при помощи CVE Editorial Board и вынесение решения о получении или неполучении индекса CVE

- **CVE кандидат**

  С кандидатом CVE ассоциируются номер, краткое описание и ссылки. Номер, также называемый именем, состоит из года и уникального индекса, например, CAN -1999-0067. После утверждения кандидатуры аббревиатура « CAN » заменяется на « CVE ».

- **CVE entry**

  После получения статуса CVE entry уязвимости присваиваются номер, краткое описание и ссылки, например, CVE -1999-0067. И затем она публикуется на сайте. Зная индекс CVE , можно быстро найти описание уязвимости и способы её устранения.

Примеры

CVE-1999-0005

- Arbitrary command execution via IMAP buffer overflow in authenticate command.
- Reference: CERT:CA-98.09.imapd
- Reference: SUN:00177. Reference: BID: 130
- Reference: XF:imap-authenticate-bo

CVE-2000-0482

- Check Point Firewall-1 allows remote attackers to cause a denial of service by sending a large number of malformed fragmented IP packets.
- Reference: BUGTRAQ:20000605 FW-1 IP Fragmentation Vulnerability
- Reference:CONFIRM:
- http://www.checkpoint.com/techsupport/alerts/list_vun#IP_Fragmentation
- Reference: BID: 1312
- Reference: XF:fw1-packet-fragment-dos

- CVE-2016-3119 (База уязвимостей http://en.securitylab.ru/nvd/)

  свойства
- Опубликовано:24.03.2016
- Обновлено:29.03.2016
- Исправление: +
- Строгость: Низкий
- CVSS вектор:(AV: N / AC: M / Au: S / C: N / I: N / A: P)
- Продукт: МИТ: Керберос
  Массачусетский технологический институт: Керберос

- Описание уязвимости

  Функция process_db_args в плагинах / KDB / Ldap / libkdb_ldap / ldap_principal2.c в LDAP KDB модуля в kadmind в MIT Kerberos 5 (он же krb5) через 1.13.4 и 1.14.1 1.14.x через mishandles аргумент DB, который позволяет удаленным пользователям, прошедшим проверку, чтобы вызвать отказ в обслуживании (указатель NULL разыменования и демон аварии) с помощью сформированного запроса для изменения основного долга.

- Рекомендации:

  Подтверждаю: https://github.com/krb5/krb5/commit/08c642c09c38a9c6454ab43a9b53b2a89b9eef99

BID

Эта классификация присутствует исключительно на портале Securityfocus (используется в ленте securityfocus.com/vulnerabilities).

Одна из отличительных особенностей BID – совместимость с CVE.

Условно говоря, найденная уязвимость в BID имеет ссылку на номер CVE и, соответственно, равнозначна по информации. У системы есть ряд описательных свойств – например, класс, возможность локального или удаленного исполнения и т.п.

Обычно этих параметров недостаточно для полной характеристики, но, тем не менее, BID дает разработчику вполне наглядную информацию о выявленной бреши.

OSVDB

Название расшифровывается примерно:

"Открытая база данных уязвимостей".

Классификация создана тремя некоммерческими организациями.

Среди прочего присутствуют: локация эксплуатации (сетевой доступ/локальный доступ) и импакт (ущерб от уязвимости, воздействие на какую-либо часть целевой информационной системы).

Secunia

Эта датская компания, лента уязвимостей которой доступна по адресу secunia.com, уже заработала себе достаточно славы. Не сказать, чтобы их портал внес какую-то особую, добавочную классификацию, но именно он предлагает услуги платной подписки на базу уязвимостей

ISS X-Force

ISS затрагивает все перечисленные выше критерии, но вдобавок описывает бизнес-импакт, а именно – материальный ущерб, который может повлечь за собой угроза эксплуатации.

Например, баг "Microsoft Excel Remote Code Execution", нацеленный на компьютер сотрудника банка или предприятия, способен привести к краже важных документов, ущерб от разглашения которых может исчисляться миллионами. Оценить урон от различных видов атак можно в русскоязычном сегменте о security-бричах и утечках — Perimetrix.

Также в системе присутствует качественно новая черта — переход к метрикам безопасности для описания свойств уязвимости. Для этого используется общая система подсчета рисков уязвимостей CVSS.

Она представляет собой шкалы, на основе которых выставляются баллы. Система метрик была придумана для разделения приоритетов над исправлением уязвимостей. Каждая шкала относится к определенному смысловому разделу, который называется метрикой.

Плюсы использования CVSS:

Стандартизованная оценка уязвимостей. После нормализации оценок уязвимостей для всех программных и аппаратных платформ компании может использоваться единая политика управления уязвимостями. Эта политика сходна с договором о предоставлении услуг (SLA, Service Level Agreement), который определяет, как быстро конкретная проблема должна быть решена.

Плюсы использования CVSS:

Открытость системы. Пользователи часто не понимают, каким образом была получена оценка уязвимости. Часто задаются такие вопросы: «Из-за каких свойств уязвимость получила именно эту оценку? Чем она отличается от той, о которой стало известно вчера?» Использование CVSS позволяет каждому увидеть индивидуальные особенности уязвимости, которые привели к указанной оценке.

Приоритезация рисков: Как только для уязвимости вычислена контекстная метрика, оценка этой уязвимости становится зависимой от среды. Это означает, что полученная оценка отражает реальный риск от наличия этой уязвимости, который существует в данной организации с учетом других уязвимостей.

Плюсы использования CVSS:

CVSS используют разные организации, и каждая получает оценки своим способом.

- Издатели бюллетеней безопасности
- Производители приложений
- Пользовательские организации
- Сканирование на уязвимости и управление уязвимостями
- Управление безопасностью(рисками)
- Исследователи

Метрики в CVSS:

- Базовая метрика:
  - представляет основные существенные характеристики уязвимости, которые не изменяются со временем и не зависят от среды.
- Временная метрика
  - представляет такие характеристики уязвимости, которые могут измениться со временем, но не зависят от среды.
- Контекстная метрика
  - представляет такие характеристики уязвимости, которые зависят от среды.

Компоненты системы, для которых рассчитываются метрики

- **Уязвимый компонент(vulnerable component)** – тот компонент информационной системы, который содержит уязвимость и подвержен эксплуатации.
- **Атакуемый компонент(impacted component)** – тот, конфиденциальность, целостность и доступность которого могут пострадать при успешной реализации атаки.

Базовая метрика

Метрики эксплуатируемости:

- **Attack Vector** (Вектор атаки) - **AV**
- **Attack Complexity** (Сложность – **AC** проведения атаки/эксплуатации уязвимости)
- **Privileges Required** (Аутентификация/требуемый уровень привилегий) - **PR**
- **User Iteration** (необходимость взаимодействия с пользователем) – UI
- **Scope** (границы эксплуатации) - **S**

Три метрики воздействия :

- **Confidentiality Impact**

(Влияние на конфиденциальность)

- **Integrity Impact**

(Влияние на целостность)

- **Availability Impack**

(Влияние на доступность)

описывают возможное прямое влияние на IT-систему в случае эксплуатации уязвимости.

Пример Базовых метрик

Уязвимость	Вектор CVSSv3	Оценка CVSSv3
CVE-2015-2363	**AV:L**/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
CVE-2015-3007	**AV:P**/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	6.8

Временные метрики

Угроза, которую несет уязвимость, может изменяться со временем.

Есть три фактора, которые изменяются со временем и учитываются в CVSS:

- подтверждение технических деталей уязвимости
- статус исправления уязвимости
- доступность кода эксплуатации или технологии эксплуатации.

Так как временные метрики являются необязательными, они не влияют на базовую оценку. Эти метрики применяются только в тех случаях, когда пользователь хочет уточнить базовую оценку.

- **Exploit Code Maturity** (**E**) –

  Возможность использования. Эта метрика отображает наличие или отсутствие кода или техники эксплуатации.

- **Remediation Level** (**RL**) –

  Уровень исправления. Наличие средств устранения уязвимости.

- **Report Confidence** (**RC**) –

  Степень достоверности отчета. Эта метрика отображает степень конфиденциальности информации о существовании уязвимости и достоверность известных технических деталей

Пример временных метрик

CVSS-вектор	Базовая оценка	Итоговая оценка
AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C	9.8	8.5

Контекстные метрики

Различные среды могут иметь огромное влияние на риск, который оказывает наличие уязвимости, для организации и заинтересованных лиц.

Группа контекстных метрик CVSS отражает характеристики уязвимости, которые связаны со средой пользователя. Так как контекстные метрики являются необязательными, они не влияют на базовую оценку. Эти метрики применяются только в тех случаях, когда пользователь хочет уточнить базовую оценку.

- **Security Requirements** (**CR, IR, AR**) - Требования к безопасности.
- **Confidentiality Requirement**
- **Integrity Requirement**
- **Avaibility Requirement**

Эти метрики позволяют аналитику определить CVSS-оценку в зависимости от важности уязвимого устройства или программного обеспечения для организации, измеренной в терминах конфиденциальности, целостности и доступности.

Качественная шкала оценки опасности

Количественная оценка	Качественная оценка
0	None
0.1—3.9	Low
4.0—6.9	Medium
7.0—8.9	High
9.0—10.0	Critical

Классификация атак

Производя атаку, злоумышленник преследует определённые цели:

- нарушение нормального функционирования объекта атаки (отказ в обслуживании)
- получение контроля над объектом атаки
- получение конфиденциальной и критичной информации
- модификация и фальсификация данных

Классификация атак по мотивации действий

- Случайность
- Безответственность
- Самоутверждение
- Идейные соображения
- Вандализм
- Принуждение
- Месть
- Корыстный интерес

Местонахождение нарушителя

Следующий возможный вариант классификации атак – по местонахождению атакующего:

- в одном сегменте с объектом атаки;
- в разных сегментах с объектом атаки.

От взаимного расположения атакующего и жертвы зависит механизм реализации атаки.

Механизмы реализации атак

- пассивное прослушивание

  Пример: перехват трафика сетевого сегмента

- • подозрительная активность

  Пример: сканирование портов (служб) объекта атаки, попытки подбора пароля

- • бесполезное расходование вычислительного ресурса

  Пример: исчерпание ресурсов атакуемого узла или группы узлов, приводящее к снижению производительности (переполнение очереди запросов на соединение и т.п.)

- • Нарушение навигации (создание ложных объектов и маршрутов)

  Пример: Изменение маршрута сетевых пакетов, таким образом, чтобы они проходили через хосты и маршрутизаторы нарушителя, изменение таблиц соответствия условных Internet -имен и IP -адресов (атаки на DNS) и т.п.

- Выведение из строя

  Пример: посыпка пакетов определённого типа на атакуемый узел, приводящая к отказу узла или работающей на нём службы.

- Запуск приложений на объекте атаки

  Пример: выполнение враждебной программы в оперативной памяти объекта атаки (троянские кони, передача управления враждебной программе путём переполнения буфера, исполнение вредоносного мобильного кода на Java или ActiveX и др.)

Для защиты от атак необходимо использовать комплекс средств безопасности, реализующий основные защитные механизмы и состоящий из следующих компонентов:

- Межсетевые экраны, являющиеся первой линией обороны и реализующие комплекс защитных механизмов, называемый защитой периметра.
- Средства анализа защищённости, позволяющие оценить эффективность работы средств защиты и обнаружить уязвимости узлов, протоколов, служб.
- Средства обнаружения атак, осуществляющие мониторинг в реальном режиме времени.

Спасибо за внимание ☺