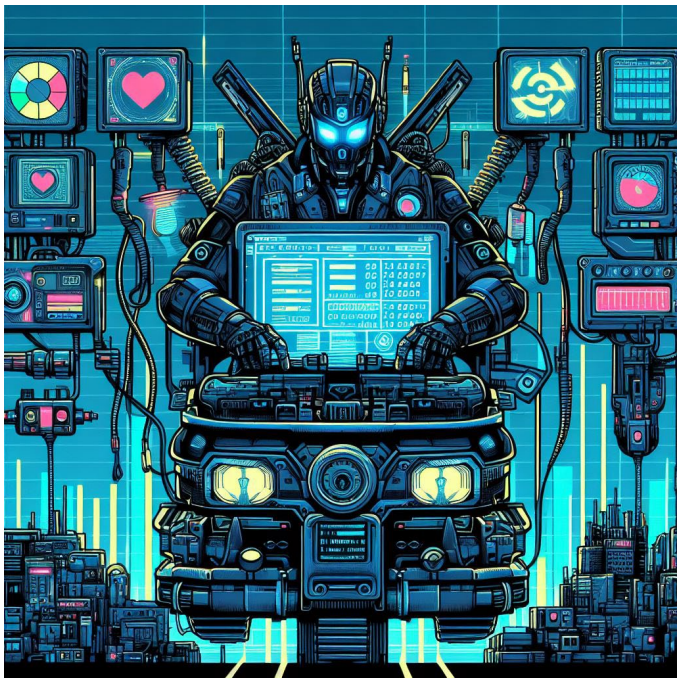

I. Введение

Общая система оценки уязвимостей (CVSS) версии 4.0 представляет собой последнюю итерацию стандартной отраслевой системы количественной оценки критичности и воздействия уязвимостей программного обеспечения.

CVSS v4.0 вносит несколько существенных изменений и улучшений по сравнению с предыдущей версией (v3.1), чтобы обеспечить более детальную, точную и всестороннюю оценку уязвимостей.

В анализе ниже будут рассмотрены различные аспекты CVSS версии 4.0, включая улучшенные показатели, введение новых категорий и последствия, которые эти изменения имеют для специалистов по кибербезопасности и организаций. Анализируя спецификацию CVSS версии 4.0, будет представлено качественное резюме, в котором собраны основные улучшения и модификации по сравнению с её предшественником, CVSS версии 3.1, что позволит читателям лучше понять её влияние на процессы управления уязвимостями. Благодаря тщательному изучению платформы CVSS версии 4.0 наряду с выводами экспертов по кибербезопасности, этот анализ направлен на то, чтобы предоставить чёткое руководство по эффективному использованию CVSS версии 4.0 для повышения уровня безопасности организации.

II. Ключевые изменения

Основные обновления в CVSS версии 4.0:

- **Новые базовые метрики и значения**: вводятся новые базовые метрики, которые отражают дополнительные аспекты риска, такие как потенциальные последствия успешной атаки, включая оценку воздействия на уязвимую систему (VC, VI, VA) и последующие системы (SC, SI, SA)
- **Упрощённые метрики угроз**: Временная оценка была переименована в Threat Metric Group и теперь включает только один показатель – зрелость
- **Новая дополнительная группа метрик**: группа введена для улучшения внешних атрибутов, дающих дополнительное представление о характеристиках уязвимости
- **Изменения в векторной строке**: Векторная строка была обновлена и теперь начинается с CVSS: 4.0, а не с CVSS: 3.1. Хотя в векторную строку не вносились никакие другие изменения, CVSS версии 4.0 содержит изменения в определении некоторых значений метрик и в формулах
- **Улучшенное руководство**: CVSS v4.0 предоставляет улучшенные рекомендации аналитикам для получения согласованных оценок, рекомендации по оценке уязвимостей в библиотеках ПО и поддерживает несколько оценок CVSS для одной и той же уязвимости, которая затрагивает разные платформы или операционные системы
- **Повышенная ясность и простота**: CVSS 4.0 нацелен на обеспечение более упорядоченного процесса расчёта, и снижения субъективности за счёт более конкретизации по метрикам
- **Акцент на отказоустойчивость**: CVSS 4.0 вновь уделяет внимание отказоустойчивости, особенно на ранних стадиях эксплойта, решая растущие проблемы, связанные с безопасностью операционных технологий (OT), промышленных систем управления (ICS) и Интернета вещей (IoT)
- **Переименование ключевых метрик**: Временные метрики в CVSS 3.1 были переименованы в метрики угроз в CVSS 4.0
- **Взаимодействие с пользователем**: CVSS 4.0 сделала показатель взаимодействия с пользователем более детализированным. В то время как в CVSS 3.1 для этого метрики были заданы значения None (N) или Required (R), в CVSS 4.0 параметры были расширены до Active, Passive и None
- **Новые базовые метрики и значения**: CVSS 4.0 вводит новые базовые метрики и значения, обеспечивая более детальную и точную оценку уязвимостей
- **Оценка воздействия на уязвимые и последующие системы**: CVSS 4.0 обеспечивает более точное представление о воздействии уязвимостей как на уязвимую систему, так и на последующие системы
- **Упрощение метрик угроз**: Метрики угроз были упрощены, чтобы сфокусироваться только на зрелости эксплойтов
- **Новая дополнительная группа метрик**: CVSS 4.0 представляет новую дополнительную группу метрик

- **Требования к атаке**: CVSS 4.0 вводит новую базовую метрику "Требования к атаке", которая получает значение "Присутствует", если есть условие предварительной атаки
- **Изменения области применения**: Функция "Области применения" из CVSS версии v3.1 была удалена и заменена понятием "Уязвимая система"
- **Поддержка нескольких оценок**: CVSS 4.0 предназначен для поддержки нескольких оценок CVSS для одной и той же уязвимости, которая затрагивает разные платформы, операционные системы и т.д.
- **Рекомендации для других секторов**: CVSS 4.0 Расширение рамок CVSS в отношении других отраслей, например, автомобилестроение.

III. Преимущества использования CVSS версии 4.0 по сравнению с предыдущими версиями

CVSS v4.0 улучшает оценку уязвимостей за счёт внедрения детального и точного представления рисков, связанных с уязвимостями программного обеспечения:

- **Более детализированные базовые метрики** – CVSS версии 4.0 включает новые базовые метрики и значения, которые отражают дополнительные аспекты риска, такие как потенциальные последствия успешной атаки. Это включает в себя чёткую оценку воздействия на Уязвимую систему (VC, VI, VA) и Последующие системы (SC, SI, SA), что позволяет получить более подробное представление о воздействии уязвимости
- **Интеграция анализа угроз** – Группа метрик угроз в CVSS версии 4.0 регулирует критичность уязвимости на основе факторов реального времени, таких как доступность кода, подтверждающего концепцию, или активное использование. Такая интеграция анализа угроз гарантирует, что оценка отражает текущий ландшафт угроз и вероятность атаки
- **Метрики окружения** – уточняют оценку критичности для конкретной вычислительной среды. Учитываются такие факторы, как наличие мер по смягчению последствий и критичность затронутой системы в среде пользователя для проведения более индивидуальной оценки рисков
- **Упрощённые метрики угроз** – Группа метрик угроз, ранее известная как Временные метрики, была упрощена, чтобы сосредоточиться на наиболее важном аспекте оценки уязвимостей в режиме реального времени - зрелости эксплойтов. Это упрощение помогает пользователям лучше понимать риск уязвимостей
- **Повышенная ясность и простота** – CVSS 4.0 направлена на уменьшение двусмысленностей и несоответствий в оценках уязвимостей, которые были распространены в предыдущих версиях. Новая версия содержит более конкретные рекомендации и определения метрик, которые должны привести к более точному подсчёту рейтинга
- **Поддержка нескольких оценок** – Новая платформа предназначена для поддержки нескольких оценок CVSS для одной и той же уязвимости, когда она затрагивает разные платформы или операционные системы, обеспечивая более полную оценку
- **Акцент на отказоустойчивость** – уделяется внимание отказоустойчивости, особенно на ранних стадиях эксплойта, что становится все более важным для безопасности операционных технологий (OT), промышленных систем управления (ICS) и Интернета вещей (IoT)
- **Предоставляемая поставщиком оценка критичности и воздействия** – теперь интегрируется предоставляемую поставщиком оценку критичности и воздействия, учитывая более широкий спектр точек зрения и более точно согласовывая процесс оценки с реальными сценариями
- **Повышенная точность оценки уязвимостей** – The Целью CVSS версии 4.0 является обеспечение повышенной точности оценки уязвимостей для отрасли и общественности, включая различные усовершенствования для повышения точности оценки уязвимостей

IV. Детализированные метрики и процесс подсчёта рейтинга

CVSS v4.0 вводит несколько более детализированных метрик для обеспечения более детального понимания технических характеристик уязвимостей. Одним из ключевых изменений является более детальная разбивка базовых метрик, которая включает новые значения для взаимодействия с пользователем, классифицируемые как Пассивные или Активные. Метрика взаимодействия с пользователем (UI) в CVSS версии 4.0 обеспечивает большую детализацию требуемого объёма взаимодействия. Кроме того, CVSS версии 4.0 вводит новую метрику требований к атаке, которая обеспечивает большую детализацию при описании предварительных условий, позволяющих атаковать.

CVSS версии 4.0 упрощает процесс оценки несколькими способами. Метрики угроз, ранее известные как временные метрики, были упрощены и переименованы, чтобы подчеркнуть важность оценки уязвимостей в режиме реального времени. Уровень исправления (RL) и достоверность отчёта (RC) были удалены, а срок действия "Кода" эксплойта был переименован в срок действия эксплойта (E). Временные метрики были упрощены, чтобы помочь потребителям лучше понять риск уязвимостей. Система оценки в CVSS версии 4.0 проще и гибче по сравнению с предыдущими версиями, цель которой - обеспечить универсальную основу для оценки различных уязвимостей.

V. Список метрик

Общая система оценки уязвимостей (CVSS) версии 4.0 состоит из четырёх групп метрик: базовые, метрики угрозы, окружения и дополнительные.

Базовая группа метрик представляет собой внутренние характеристики уязвимости, которые остаются постоянными с течением времени и в разных пользовательских средах. Базовый балл рассчитывается по специальной формуле, которая учитывает такие факторы, как влияние уязвимости на целостность, конфиденциальность, доступность, возможность использования и масштаб.

Группа метрик угроз, ранее известная как группа временных метрик, предоставляет дополнительный контекст для базовых метрик. Однако метрики угроз не оказывают существенного влияния на итоговую оценку CVSS.

Группа метрик окружения представляет характеристики уязвимости, которые являются уникальными для среды пользователя. Эти метрики позволяют организациям настраивать метрики CVSS на основе их конкретной среды. Однако метрики состояния окружения определяются пользователями и напрямую не влияют на общедоступные оценки CVSS, которые основаны исключительно на Базовой оценке.

Дополнительная группа метрик — это новое дополнение в CVSS версии 4.0. В неё входят метрики, обеспечивающие дополнительный контекст, такие как автоматизируемость, восстановление, срочность для поставщика и усилия по устранению уязвимостей. Однако дополнительные метрики являются необязательными и не оказывают никакого влияния на окончательный расчётный балл CVSS.

A. Базовые метрики

Базовые метрики представляют собой неотъемлемые качества уязвимости:

- Вектор атаки (AV)
- Сложность атаки (AC)
- Требуемые привилегии (PR)
- Взаимодействие с пользователем (UI)
- Область применения
- Метрики воздействия: Конфиденциальность уязвимой системы (VC), Целостность (VI), Доступность (VA) и Системные Конфиденциальность (SC), Целостность (SI), Доступность (SA)

1) Цель

Базовая группа метрик представляет собой внутренние качества уязвимости, которые остаются постоянными с течением времени. Она состоит из двух наборов метрик: метрик возможности использования и метрик воздействия. Метрики эксплуатируемости отражают простоту и технические средства, с помощью которых уязвимость может быть использована, в то время как метрики воздействия отражают прямые последствия успешного эксплойта. Базовые метрики помогают определить начальную оценку критичности уязвимости. В CVSS версии v3.1 базовая группа метрик состояла из четырёх основных метрик: вектор атаки (AV), Сложность атаки (AC), Требуемые привилегии (PR) и взаимодействие с пользователем (UI). В CVSS 4.0 введён показатель, называемый Требованиями к атаке (AT), для повышения детализации системы подсчёта рейтинга

2) Влияние на оценку

Базовые метрики дают оценку в диапазоне от 0 до 10, которую затем можно изменить, оценив метрики угрозы и окружения. Базовая оценка отражает техническую критичность уязвимости только при рассмотрении ее отдельно. Важно отметить, что базовый балл является лишь отправной точкой для построения полной картины риска, связанного с уязвимостью.

3) Использование

Базовая группа метрик используется для оценки фундаментальных качеств уязвимости, которые сохраняют своё постоянство с течением времени. Он используется для оценки критичности уязвимостей и их влияния на организации без учёта временных метрики или окружения

4) Расчёт

Базовые метрики делятся на метрики эксплуатируемости и метрики воздействия. Когда аналитик присваивает этим базовым метрикам значения, они дают оценку в диапазоне от 0.0 до 10.0.

Калькулятор CVSS версии 4.0, который является эталонной реализацией стандарта CVSS, может использоваться для генерации оценок на основе значений этих метрик. Калькулятор применяет формулу, указанную в стандарте CVSS версии 4.0, для получения базового балла

5) Ропределение приоритетов уязвимостей

Базовые метрики представляют собой внутренние характеристики уязвимости, которые остаются постоянными с течением времени и в разных пользовательских средах. Они включают метрики возможности использования (такие как вектор атаки, сложность атаки, требования к атаке, требуемые привилегии и взаимодействие с пользователем) и метрики воздействия на уязвимую систему (такие как конфиденциальность, целостность и доступность) и последующие метрики воздействия на систему. Базовые метрики дают оценку в диапазоне от 0 до 10, которая отражает техническую критичность уязвимости, если рассматривать ее изолированно. Этот показатель важен при анализе уязвимости и помогает определить приоритеты уязвимостей на основе присущих им характеристик

B. Метрики угроз

Метрики угроз, ранее известные как Временные метрики, корректируют критичность уязвимости на основе факторов реального времени. К ним относятся:

- Зрелость использования (E)
- Уровень восстановления (RL)

- Достоверность отчета (RC)

1) Цель

Цель группы метрик угроз – скорректировать критичность уязвимости на основе таких факторов, как доступность кода, подтверждающего концепцию, или активное использование. Эта группа отражает характеристики уязвимостей, связанные с угрозой, которые могут меняться с течением времени.

Например, он включать такую информацию, использовалась ли уязвимость или существует ли какой-либо подтверждающий концепцию эксплойт. Значения, найденные в этой группе метрик, могут меняться с течением времени, отражая меняющийся ландшафт угроз.

2) Влияние на оценку

Группа метрик угроз влияет на итоговую оценку CVSS, корректируя критичность уязвимости в зависимости от ландшафта угроз. Отсутствие явных выбранных метрик угрозы все равно приведёт к получению балла, но включение “T” в номенклатуру уместно, если какие-либо метрики угрозы используются для корректировки балла

3) Использование

Группа метрик угроз используется для уточнения оценки критичности уязвимости на основе применимого анализа угроз. Он используется в сочетании с группой базовых метрик, которая представляет внутренние качества уязвимости, которые остаются постоянными с течением времени, и группой метрик среды, которая представляет характеристики уязвимости, уникальные для конкретной вычислительной среды.

4) Расчёт

Метрики угроз в Общей системе оценки уязвимостей (CVSS) версии 4.0 корректируют критичность уязвимости на основе таких факторов, как доступность кода, подтверждающего концепцию, или активное использование. Эти метрики отражают характеристики уязвимости, связанные с угрозой, которые могут меняться с течением времени.

В CVSS версии 4.0 метрики угроз заменили временные метрики из предыдущих версий, что привело к более конкретным и упрощённым метрикам. Метрики уровня исправления (RL) и достоверности отчёта (RC), которые были частью временных метрик в предыдущих версиях, были удалены в CVSS версии 4.0.

Значения, присвоенные метрикам угрозы, используются при расчёте окончательной оценки наряду с базовыми метриками и метриками окружения. Если явные значения метрик угрозы не предоставлены, используются значения по умолчанию, которые предполагают наибольшую критичность.

Калькулятор CVSS версии 4.0, который является эталонной реализацией стандарта CVSS, может использоваться для генерации оценок на основе значений этих метрик. Калькулятор применяет формулу, указанную в стандарте CVSS версии 4.0, для получения окончательной оценки, которая включает метрики угрозы.

5) Определение приоритетов уязвимостей

Метрики угроз, ранее известные как временные метрики, корректируют критичность уязвимости на основе таких факторов, как доступность кода, подтверждающего концепцию, или активное использование. Эти метрики отражают характеристики уязвимости, которые меняются с течением времени, например, использовалась ли уязвимость или существует ли какой-либо подтверждающий концепцию эксплойт. Значения в этой группе метрик могут меняться с течением времени, и они помогают в оценке уязвимости в режиме реального времени. Принимая во внимание вероятность использования и потенциальное воздействие успешной атаки, CVSS версии 4.0 стремится предложить более целостную и точную оценку уязвимостей.

C. Метрики окружения

Метрики окружения позволяют организациям настраивать метрики CVSS на основе их конкретной среды. Они включают:

- Измененные Базовые метрики
- Потенциальный сопутствующий ущерб (CDP)
- Метрики требований к безопасности: Требования к конфиденциальности уязвимой системы (CR), Требования к целостности уязвимой системы (IR) и требования к доступности уязвимой системы (AR)

1) Цель

Группа метрик среды в CVSS версии 4.0 представляет характеристики уязвимости, уникальные для среды пользователя. Это позволяет организациям корректировать Базовую оценку уязвимости, чтобы отразить ее влияние в их конкретном контексте. Эта группа объясняет наличие средств контроля безопасности, которые могут смягчить некоторые или все последствия уязвимости, и относительную важность уязвимой системы в технологической инфраструктуре.

2) Влияние на оценку

Метрики окружения позволяют аналитикам настраивать оценку CVSS с учётом исходных данных, касающихся важности ИТ-активов и наличия мер по смягчению последствий, которые могут увеличить или уменьшить критичность уязвимости. Эти метрики являются модификаторами базовой группы метрик и предназначены для учёта аспектов деятельности предприятия, которые могут влиять на критичность уязвимости. Группа метрик окружения влияет на итоговую оценку CVSS, позволяя вносить коррективы в зависимости от конкретной среды, в которой существует уязвимость.

3) Использование

Группа метрик окружения используется для адаптации метрики CVSS к уникальной среде организации с учётом таких факторов, как важность затронутого ИТ-актива и эффективность существующих средств контроля безопасности. Эти метрики являются модифицированным эквивалентом Базовых метрик и задаются пользователями для обеспечения более точной оценки риска, связанного с уязвимостью, в их конкретном операционном контексте.

4) Расчёт

Метрики окружения в Общей системе оценки уязвимостей (CVSS) версии 4.0 предназначены для корректировки базовой оценки уязвимости с учётом воздействия в конкретном организационном контексте. Эти метрики учитывают цели защиты уязвимой системы и наличие средств контроля безопасности, которые уменьшают уязвимость.

Метрики рассчитываются путём предварительного определения Модифицированных базовых метрик, которые представляют собой Базовые метрики, скорректированные с учётом наличия мер по смягчению последствий или компенсирующих средств управления. Требования безопасности используются для указания важности затронутого ИТ-ресурса для организации, что может усилить или уменьшить критичность в зависимости от критичности актива. Показатель потенциального сопутствующего ущерба отражает потенциальный непрямой ущерб, выходящим за рамки ИТ-активов.

Окончательная оценка окружения рассчитывается путём объединения модифицированных базовых метрик с требованиями безопасности и потенциальным сопутствующим ущербом с использованием формулы из спецификации CVSS v4.0. Этот показатель обеспечивает индивидуальную оценку критичности уязвимости в конкретной среде организации

5) Определение приоритетов уязвимостей

Метрики окружения дополнительно уточняют результирующий показатель критичности для конкретной вычислительной среды. Они учитывают такие факторы, как наличие мер по смягчению последствий в этой среде и критичность систем. Эти метрики задаются пользователями и могут привести к расхождению между оценкой и фактическим риском в реальном мире из-за их субъективного характера. Однако они имеют решающее значение для обеспечения более точной оценки уязвимостей в конкретной среде, тем самым улучшая определение приоритетов уязвимости и управление рисками.

D. Дополнительные метрики

Дополнительные метрики предоставляют дополнительный контекст и описывают аспекты уязвимости, которые выходят за рамки основного стандарта CVSS. К ним относятся:

- Автоматизируемость (A)
- Контроль над ресурсами (VD)
- Восстановление ®
- Срочность устранения (PU)
- Усилия по реагированию на уязвимости (VRE)

1) Цель

Цель Дополнительной группы метрик - предоставить пользователям контекстуальную информацию, позволяющую более детально разобраться в уязвимостях. Эти метрики дают ценную информацию о внешних аспектах уязвимостей, позволяя потребителям глубже вникать в конкретные контекстуальные соображения. Они предназначены для обеспечения более полного понимания уязвимостей путём описания и измерения дополнительных внешних атрибутов

2) Влияние на оценку

В отличие от основных метрик CVSS, Дополнительные метрики не участвуют в расчёте рейтинга CVSS. Они не оказывают никакого влияния на окончательный расчётный балл CVSS. Вместо этого они служат дополнительной информацией для более детальной оценки уязвимости. Затем организации могут присвоить важность и /или эффективное влияние каждой метрике или набору / комбинации метрик, оказывая им большее, меньшее или абсолютно нулевое влияние на конечный анализ рисков

3) Использование

Использование каждой метрики в группе дополнительных метрик определяется потребителем оценки. Эта контекстуальная информация может использоваться по-разному в среде каждого потребителя. Затем потребитель информации может использовать значения этих Дополнительных метрик для выполнения дополнительных действий, если он того пожелает, придавая метрикам и значениям локальную значимость.

4) Расчёт

Дополнительные метрики в Общей системе оценки уязвимостей (CVSS) версии 4.0 являются новым дополнением, разработанным для предоставления дополнительного контекста и описания внешних атрибутов уязвимости. Эти метрики необязательны и не участвуют в расчёте окончательной оценки CVSS. Вместо этого они служат дополнительной информацией для более детальной оценки уязвимости.

План использования и реагирования на каждую метрику в группе дополнительных метрик определяется пользователем, проводящим оценку. Эта контекстуальная информация может использоваться по-разному в среде каждого пользователя. Затем организации могут присвоить важность и / или эффективное влияние каждой метрике или набору / комбинации метрик, оказывая им большее, меньшее или абсолютно нулевое влияние на окончательный анализ рисков.

5) Ропределение приоритетов уязвимостей

Дополнительные метрики являются новым дополнением в CVSS версии 4.0. Они измеряют внешние атрибуты уязвимости и предоставляют контекстуальную информацию. Эти метрики не влияют на оценку уязвимости, но могут быть использованы для информирования компаний, приобретающих продукты для обеспечения дополнительного контекста для групп по уязвимости и устранению последствий

E. Различия

Дополнительная группа метрик используется для предоставления дополнительного контекста и не влияет на оценку CVSS, в то время как группы метрик базы, угрозы и окружения вносят непосредственный вклад в процесс

оценки и необходимы для расчёта критичности уязвимости. Группа дополнительных метрик в CVSS версии 4.0 отличается от групп базовых метрик, метрик угроз и метрик окружения несколькими способами:

Дополнительная группа метрик:

- **Назначение**: предоставляет дополнительный контекст и описывает внешние атрибуты уязвимости, которые выходят за рамки основного стандарта CVSS
- **Влияние на оценку**: Метрики в этой группе не влияют на окончательный расчётный балл CVSS. Они являются необязательными и используются для передачи дополнительной информации, которая может повлиять на анализ рисков организации и план реагирования
- **Использование**: Использование и план реагирования для каждой метрики в группе дополнительных метрик определяются пользователем, проводящим оценку, и эта контекстуальная информация может использоваться по-разному в среде каждого потребителя

Базовые группы метрик, угрозы и окружения:

- **Назначение**: Эти группы содержат метрики, которые непосредственно вносят вклад в расчёт метрики CVSS, отражающего внутренние характеристики уязвимости (Базовый уровень), ландшафт угроз в реальном времени (Угроза) и конкретное воздействие в контексте организации (окружение)
- **Влияние на оценку**: Метрики в этих группах напрямую влияют на итоговую оценку CVSS, причём каждая группа по-разному оценивает критичность и влияние уязвимости
- **Использование**: Базовые метрики предоставляются организацией, обслуживающей уязвимую систему, или третьей стороной, в то время как метрики угроз и окружение предназначены для конечных потребителей, чтобы дополнить базовые метрики дополнительным контекстом

VI. Метрики воздействия различных технологий

В CVSS версии 4.0 были введены новые метрики для учёта выявления уязвимостей в операционных технологиях (OT) и их воздействия. Эти метрики особенно актуальны в связи с растущей озабоченностью по поводу безопасности OT, промышленных систем управления (ИС) и Интернета вещей (IoT). Обновления направлены на обеспечение более точной оценки рисков, связанных с уязвимостями в этих средах

A. Метрики безопасности

Метрики безопасности были добавлены как в группы дополнительных метрик, так и в группы метрик окружения в CVSS версии 4.0. Эти метрики оценивают потенциальное влияние использования уязвимости на безопасность, что особенно важно в таких секторах, как здравоохранение или промышленные системы управления, где безопасность является критической проблемой

B. Особые соображения, связанные с OT

Новые метрики воздействия эксплуатационных технологий включают в себя соображения о том, соответствуют «и "последствия уязвимости определению IEC 61»08", который является стандартом функциональной безопасности систем, связанных с электрической / электронной / программируемой электроникой. Это включение отражает растущую озабоченность по поводу кибер-рисков OT и потребность в системе оценки, которая может адекватно отражать уникальные риски, связанные с средами OT

C. Воздействие на Уязвимые и Последующие системы

В CVSS версии 4.0 также особое внимание уделяется оценке воздействия эксплуатации уязвимости как на уязвимую систему, так и на последующие системы. Это особенно актуально для операционных сред, где уязвимость в одном компоненте потенциально может оказывать каскадное воздействие на другие взаимосвязанные системы

D. Использование дополнительных метрик и метрик окружения

Хотя Дополнительные метрики напрямую не влияют на итоговую оценку CVSS, они предоставляют ценную контекстуальную информацию, которая может быть использована организациями для обоснования своего анализа рисков и планов реагирования. Метрики окружения позволяют настраивать оценки CVSS на основе конкретной среды, которая может включать в себя другие настройки