УДК 004.056.5(045)

ИССЛЕДОВАНИЕ БАЗ ДАННЫХ УЯЗВИМОСТЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Александр Корченко, Светлана Казмирчук, Алиреза Арджомандифард, Татьяна Панивко

Существующие общедоступные базы данных уязвимостей хранят в себе различные данные об известных уязвимостях ресурсов информационных систем. Описания уязвимостей содержат как предусловия, так и оценки, характеризующие результат реализации атак, эксплуатирующих эти уязвимости. Часто перед специалистами, занимающимися исследованием состояния безопасности информационных систем, возникает вопрос о выборе соответствующих баз данных. Эти базы, относительно определенных критериев, могут эффективно использоваться для построения различных систем оценивания состояния информационной безопасности, например, систем оценивания рисков. В связи с этим исследован широкий спектр соответствующих баз данных и определенны критерии, по которым можно осуществить их сравнительный анализ. Это даст возможность повысить эффективность решения задач оценивания состояния безопасности ресурсов информационных систем.

Ключевые слова: *база данных уязвимостей, оценивание уязвимостей, ресурсы информационных систем, информационная безопасность, анализ баз данных уязвимостей.*

При построении различных систем защиты информации (ЗИ) (например, систем менеджмента информационной безопасности (ИБ) [13] или комплексных систем ЗИ [5]) возникает необходимость осуществлять оценивание состояния ИБ, с учетом известных уязвимостей ресурсам информационных систем (РИС). Поэтому перед специалистами, занимающимися исследованием состояния безопасности информационных систем (ИС), возникает вопрос о эффективности использования соответствующих баз данных (БД) уязвимостей, удовлетворяющих определенным критериям [4, 6-9], таким, например, как наличие идентификаторов CVE, оценок CVSS, CWE категорий, CVSS-калькулятора, риск-калькулятора и д.р. Использование указанных критериев позволит осуществить рациональный выбор таких БД. В связи с этим актуальной является задача исследования соответствующих БД для определения набора критериев, согласно которых можно эффективно использовать такие базы.

На сегодняшний день существует широкое множество общедоступных БД уязвимостей РИС, которые подвергались анализу в различных источниках. Так, в работе [7] проводилось исследование открытых БД уязвимостей, где авторами были определены основные поля записей уязвимостей, достоинство и недостатки рассматриваемых баз, но не определенны обобщенные критерии, по которым можно осуществлять такой анализ. Также в работах [2, 8, 9] рассмотрены БД с точки зрения наличия ссылок на другие базы, возможности получения информации в формате XML, а также формате представления уязвимостей в БД. Следует отметить, что в [2, 8] не определены четкие критерии, по которым можно осуществить соответствующий анализ. Авторами работы [9], при обосновании выбора БД, за основу были приняты следующие критерии: полнота (емкость, количество уязвимостей); доступность данных (бесплатная база); удобство получения данных (интерфейсы); поддержка оценки уязвимостей по системе CVSS, но больше делался акцент на уязвимости, влияющие на доступность. Также следует отметить, что в работах [2, 4, 6-9] не были четко выделены критерии, по которым можно было сравнить БД уязвимостей и осуществить их выбор для построения различных систем оценивания в области ИБ, например, таких как системы анализа и оценивании рисков.

В связи с этим, целью данной работы является исследование широкого спектра существующих БД уязвимостей для определения критериев, по которым можно осуществить сравнительный анализ таких баз и использовать их при анализе и оценивании рисков ИБ.

Для проведения такого исследования, воспользуемся наиболее известными и общедоступными БД уязвимостей: национальная БД уязвимостей – National Vulnerability Database (NVD), (США) [15]; банк данных угроз безопасности информации (Российская Федерация) [1]; открытая БД уязвимостей – Open Sourced Vulnerability Database (OSVDB), (США) [16]; БД уязвимостей IBM X-Force, (США) [13]; БД записей уязвимостей US-CERT – Vulnerability Notes Database US-CERT (VND), (США) [19]; БД уязвимостей SecurityFocus, (США) [18]. Рассмотрим каждую из них.

National Vulnerability Database. База разработана National Institute of Standards and Technology (NIST) Computer Security Division, Information Technology Laboratory при поддержке De-

partment of Homeland Security's National Cyber Security Division. Она является государственным хранилищем данных США, которое основано на стандартах управления уязвимостями. Такие данные позволяют автоматизировать процессы управления уязвимостями, измерять состояние ИБ и определять его соответствие. База NVD включает в себя БД контрольных списков безопасности, недостатков РИС, неправильных конфигураций, РИС и показателей воздействия.

Рассматриваемая БД представляет собой репозитарий основных стандартов управления данными уязвимостей, разработанный на основе протокола автоматизации контента безопасности – Security Content Automation Protocol (SCAP) [15]. Существуют следующие компоненты SCAP: БД уязвимостей безопасности – Common Vulnerabilities and Exposures (CVE); БД уязвимых конфигураций РИС – Common Configuration Enumeration (CCE); стандартная номенклатура и база имен РИС – Common Platform Enumeration (CPE); БД слабых мест – Common Weakness Enumeration (CWE); стандарт оценки влияния уязвимостей – Common Vulnerability Scoring System (CVSS); стандарт XML-спецификации контрольных листов –Extensible Configuration Checklist Description Format (XCCDF); стандарт XML-спецификации контроля состояний процессов – Open Vulnerability and Assessment Language (OVAL) [15]. Кроме этого применяется следующий набор других протоколов.

Threat Analysis Automation Protocol (TAAP) – протокол документирования и совместного использования структурной информации об угрозах. Он содержит следующие компоненты: БД атрибутов вредоносного программного обеспечения (ПО) – Malware Attribute Enumeration & Characterization (MAEC); БД шаблонов атак – Common Attack Pattern Enumeration & Classification (CAPEC); CPE; CWE; OVAL; CCE; CVE.

Event Management Automation Protocol (EMAP) – протокол для отчетов о событиях безопасности. Он имеет следующие составляющие: БД записей событий – Common Event Expression (CEE); MAEC; CAPEC.

Incident Tracking and Assessment Protocol (ITAP) – протокол для отслеживания, документирования, управления и совместного использования информации об инцидентах. Он содержит следующие компоненты: OVAL; CPE; CCE; CVE; CVSS; MAEC; CAPEC; CWE; CEE; формат обмена описанием инцидента – Incident Object Description Exchange Format (IODEF); национальная модель обмена информацией – National Information Exchange Model (NIEM); формат обмена информацией по кибербезопасности – Cybersecurity Information Exchange Format (CYBEX) [15].

Рассмотренные протоколы, стандарты и базы данных NVD на практике, например, можно использовать в следующих целях: CPE – определение ИС предприятия; CVE – идентификация уязвимостей; CVSS – определение критичных уязвимостей; CCE – формирование наиболее защищенной конфигурации ИС; XCCDF – определение политики защищенной конфигурации; OVAL – оценка соответствия системы политике защищенной конфигурации; CWE – определение слабых мест РИС; CAPEC – определение атак относительно слабых мест РИС; CEE – определение событий для регистрации и параметров регистрации; ARF – объединение результатов оценки; MAEC – определение вредоносного ПО. Следует отметить, что в NVD вычисляется индекс рабочей нагрузки на информацию I_W, который показывает количество критических уязвимостей. Чем выше число, тем больше нагрузка на систему безопасности. Индекс нагрузки NVD рассчитывается по следующей формуле: $I_W = (N_h + (N_m / 5) + (N_l / 20)) / 30$, где N_h, N_m и N_l – количество уязвимостей с высокой, средней и низкой степенью тяжести соответственно, которые были опубликованы в течении последних 30 дней. Как видно из формулы одна уязвимость высокой степени тяжести приравнивается к пяти уязвимостям со средней и двадцати с низкой степенью тяжести [15]. На сайте NVD доступен полный список уязвимостей содержащихся в базе, который отсортирован по годам и месяцам (см. рис. 1).

Каждая уязвимость, вносимая в БД, описывается следующим набором параметров (рис. 2): уникальный CVE-идентификатор; даты внесения в БД; дата последней редакции; источник уязвимости (информации); краткое описание (обзор); результаты оценок по каждой метрике CVSS (см. рис. 2, 3 и табл. 1) – базовой (Base Score), временной (Temporal Score) и контекстной (Environmental Score). В БД CVSS доступен в двух версиях – v2.0 [10] и v3.0 [11]; уязвимые версии ПО; CWE категория; дополнительные ссылки; другие сведения [15]. Отметим, что условие существования уязвимости хранится в виде дизъюнктивной нормальной формы. Рассмотрим более детально каждую из версий CVSS и определим их отличия.

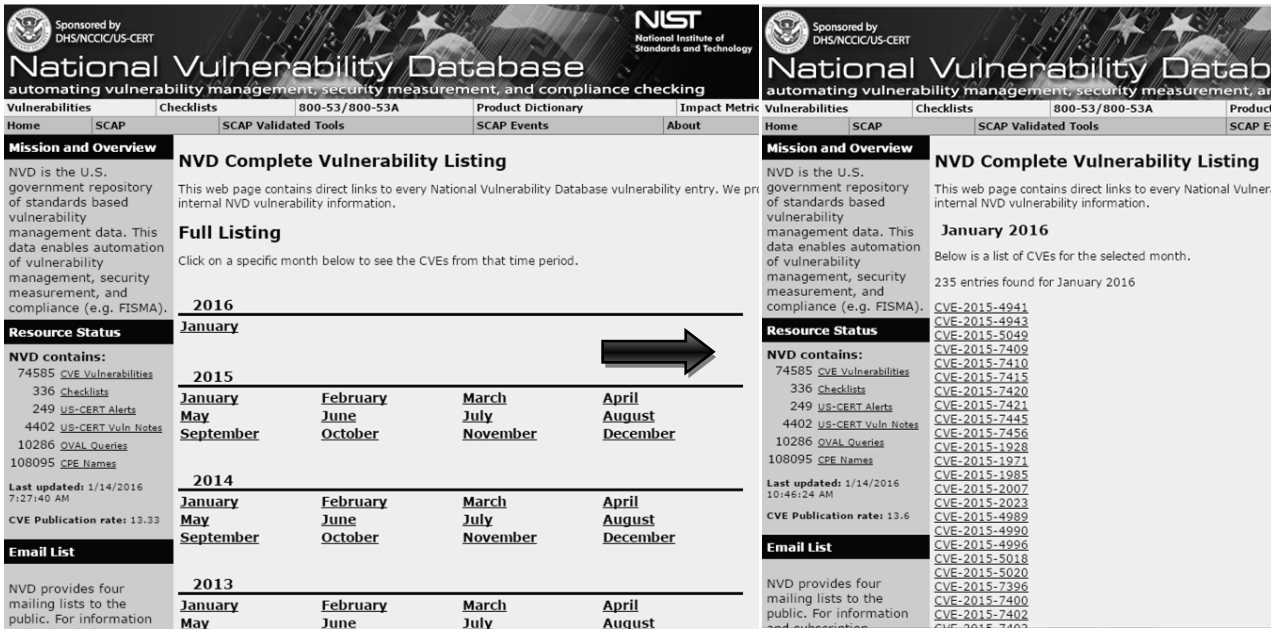


Рис. 1. Список уязвимостей на сайте NVD

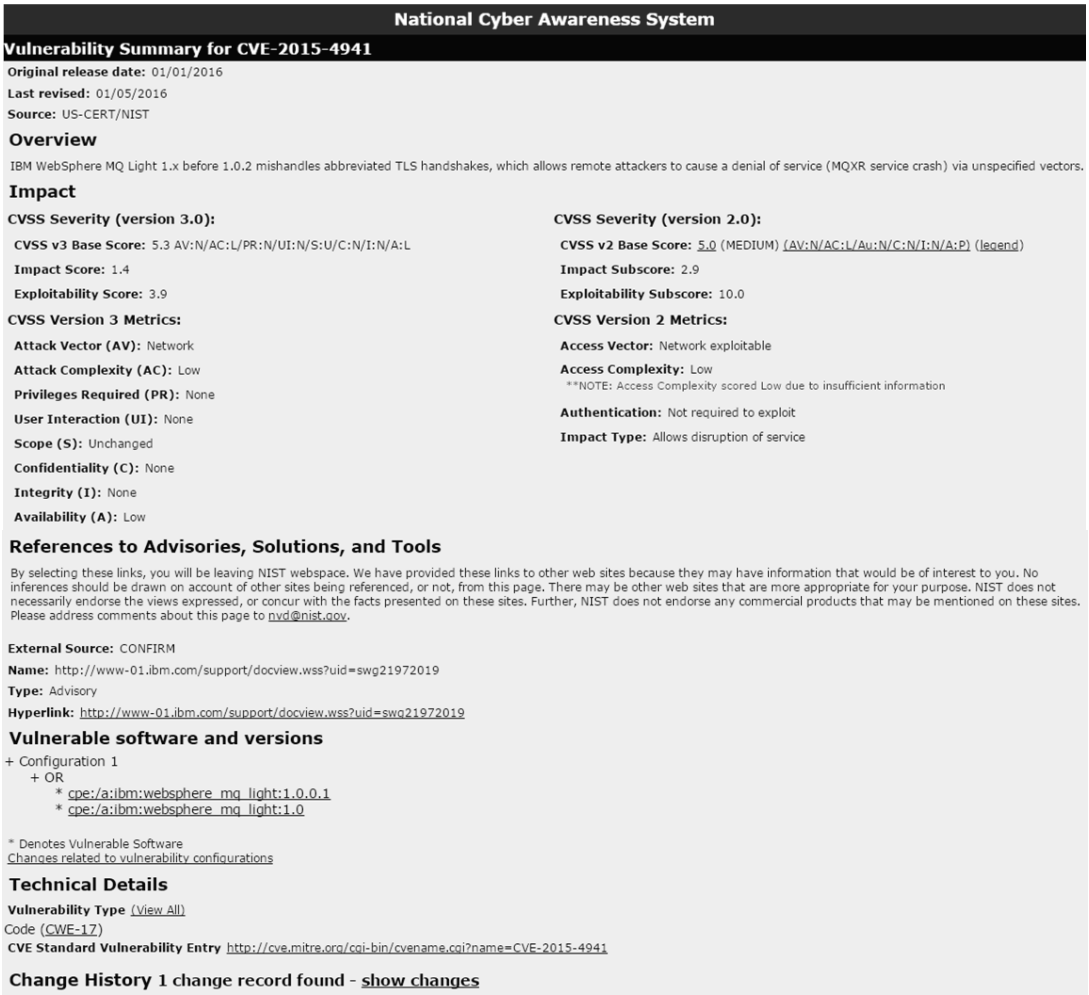


Рис. 2. Пример представления уязвимости в NVD

CVSS v2.0. Метрики и их параметры, входящие в стандарт CVSS v2.0 [10] показаны на рис. 3. В этой версии осуществляется стандартизированное оценивание уязвимостей, система является открытой и ориентирована она определение приоритетных рисков. Каждая метрическая группа (МГ) определяет характеристики уязвимости. Опишем эти группы (см. рис. 3).

Base Score Metrics (метрики базовых оценок) – характеристики уязвимостей, являющиеся постоянными в течение большого периода времени в пользовательских средах и не зависящие

от них. Также они описывают сложность эксплуатации уязвимости и потенциальный ущерб для конфиденциальности, целостности и доступности. Используемые МГ состоят из следующих показателей: вектор доступа (Access Vector (**AV**)); сложность доступа (Access Complexity (**AC**)); аутентификация (Authentication (**Au**)); воздействие на конфиденциальность (Confidentiality Impact (**C**)); воздействие на целостность (Integrity Impact (**I**)); воздействие на доступность (Availability Impact (**A**)).

Рис. 3. МГ CVSS v2.0

Temporal Score Metrics (метрики временных оценок) – характеристики уязвимости, которые изменяются с течением времени, вне пользовательских сред. Они вносят в общую оценку поправку на полноту имеющейся информации об уязвимости, зрелость эксплуатируемого кода (при его наличии) и доступность исправлений. Ее показатели: возможность использования (Exploitability (**E**)); уровень исправления (Remediation Level (**RL**)); достоверность отчета (Report Confidence (**RC**)).

Таблица 1

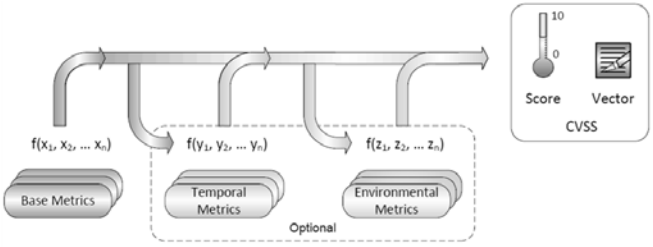
Значения показателей оценок CVSS v2.0

МГ	Множество показателей	Наборы символьных значений показателей	Числовые значения соответствующих показателей
Базовая	**AV**	L; A; N	0,395; 0,646; 1
	AC	H; M; L	0,35; 0,61; 0,71
	Au	M; S; N	0,45; 0,56; 0,704
	C; I; A	N; P; C	0; 0,275; 0,66
Временная	**E**	ND; U; POC; F; H	1; 0,85; 0,9; 0,95; 1
	RL	ND; OF; TF; W; U	1; 0,87; 0,9; 0,95; 1
	RC	ND; UC; UR; C	1; 0,90; 0,95; 1
Среды окружения	**CDP**	ND; N; L; LM; MH; H	0; 0; 0,1; 0,3; 0,4; 0,5
	TD	ND; N; L; M; H	1; 0; 0,25; 0,75; 1
	CR; IR; AR	ND; L; M; H	1; 0,5; 1; 1,51

Environmental Score Metrics (метрики контекстных оценок) – характеристики уязвимости, которые актуальны и уникальны для среды конкретного пользователя. При помощи этих метрик эксперты по безопасности могут внести в результирующую оценку поправки с учетом характеристик информационной среды. Группа МГ состоит из показателей общих модификаторов (General Modifiers) – возможность косвенного ущерба (Collateral Damage Potential (**CDP**)), целераспределение (Target Distribution (**TD**)) и модификаторов влияющих показателей (Impact Subscore Modifiers) – требование конфиденциальности (Confidentiality Requirement (**CR**)), требование целостности (Integrity Requirement (**IR**)), требование доступности (Availability Requirement (**AR**)).

В таблице 1 для каждой МГ (метрикам оценок) по каждому множеству показателей приведены наборы символьных значений и соответствующие им числовые показатели. Здесь, каждому символьному значению определена соответствующая ему лингвистическая интерпретация – для **AV** (Access Vector – вектор доступа): L – «Локальный доступ»; A – «Сопряженная сеть»; N – «Сеть», для **AC** (Access Complexity – сложность доступа): H – «Высокая»; M – «Средняя»; L – «Низкая», для **Au** (Authentication – аутентификация): M – «Многоразовая»; S – «Одноразовая»; N – «Отсутствует», для **C** (Confidentiality Impact – воздействие на конфиденциальность), **I** (Integrity Impact – воздействие на целостность), **A** (Availability Impact – воздействие на доступность): N – «Отсутствует»; P – «Частичное»; C – «Полное», для **E** (Exploitability – возможность использования): ND – «Не определенна»; U – «Теоретическая (нет доказательств)»; POC – «Экспериментальная»; F – «Функциональная»; H – «Высокая», для **RL** (Remediation Level – уровень исправления): ND – «Не определен»; OF – «Официальный патч»; TF – «Временное решение»; W – «Решение на основе советов и рекомендаций»; U – «Отсутствует», для **RC** (Report Confidence – достоверность отчета): ND – «Не определенна»; UC – «Носит предположительный характер»; UR – «Не проработана»; C – «Подтверждена», для **CDP** (Collateral Damage Potential – возможность косвенного ущерба): ND – «Не определенна»; N – «Отсутствует»; L – «Низкая»; LM – «Низко – средняя»; MH – «Средне – высокая»; H – «Высокая», для **TD** (Target Distribution – целераспределение): ND – «Не определено»; N – «Отсутствует»; L – «Низкое»; M – «Среднее»; H – «Высокое», для **CR**

(Confidentiality Requirement – требование конфиденциальности), **IR** (Integrity Requirement – требование целостности), **AR** (Availability Requirement – требование доступности): ND – «Не определено»; H – «Высокое»; M – «Среднее»; L – «Низкое» (также см. рис. 3 и 4).

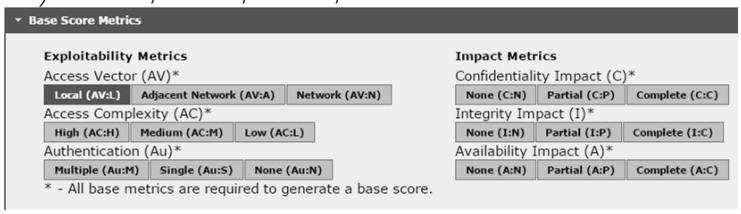


Metric Group	Vector
Base	AV:[L,A,N]/AC:[H,M,L]/Au:[M,S,N]/C:[N,P,C]/I:[N,P,C]/A:[N,P,C]
Temporal	E:[U,POC,F,H,ND]/RL:[OF,TF,W,U,ND]/RC:[UC,UR,C,ND]
Environmental	CDP:[N,L,LM,MH,H,ND]/TD:[N,L,M,H,ND]/CR:[L,M,H,ND]/ IR:[L,M,H,ND]/AR:[L,M,H,ND]

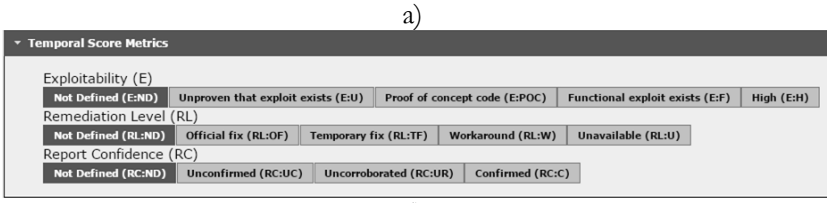
Рис. 4. CVSS v2.0 – МГ и вектора

После присвоения символьным значениям конкретных чисел, осуществляется вычисление рейтинга (в приделах [0; 10]) и создание вектора (как показано на рис. 2) AV:N/ AC:L/ Au:N/ C:N/ I:N/ A:P, который отображает «открытость» структуры. Фактически, это текстовая строка, которая содержит значения, присвоенные каждой метрике и используется для взаимодействия оценок. Отметим, что таким образом, вектор должен отображаться с учетом уязвимости [10].

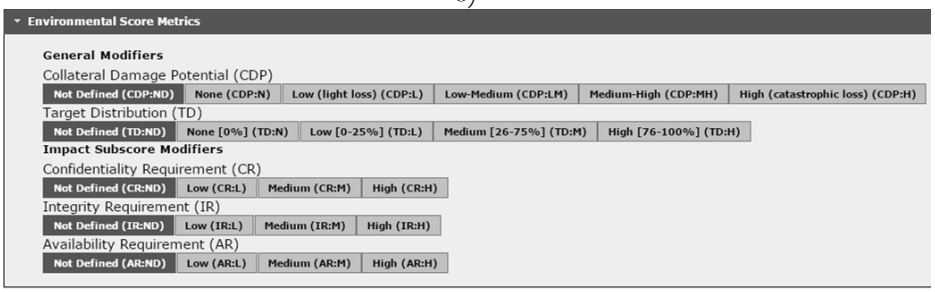
Временные и контекстные МГ опциональны и применяются для более точной оценки опасности, которую представляет данная уязвимость для конкретной инфраструктуры. Значение МГ отображается в виде пары (см. рис. 4) из вектора (конкретные значения отдельных показателей) и числового значения, рассчитанного на основе всех показателей посредством формул стандарта [10]. Использование Temporal позволяет объединить временные и базовые показатели, отображаемые на шкалу с пределами [0; 10]. При этом временная оценка будет не выше базовой, но не меньше ее на 33% [10]. На рис. 5 показан встроенный калькулятор показателей CVSS v2.0 в Веб-интерфейс NVD [15].



а)



б)



в)

Рис. 5. Интерфейс встроенного калькулятора CVSS v2.0 в Веб-интерфейс NVD
МГ: а) Базовая, б) Временная, в) Среды окружения

CVSS v3.0. Калькулятор CVSS v3.0 является развитием CVSS v2.0. На рис. 6 в виде примера, схематически показаны изменения, внесенные в третью версию. Например, рассмотрим уязвимость в виртуальной машине, подвергающую угрозе основную операционную систему (ОС). Здесь уязвимым компонентом является виртуальная машина, а влияющим компонентом – ОС хоста. Это связано с тем, что эти два компонента независимо управляют правами на вычислительные ресурсы. Виртуальная машина (как показано на рис. 6) управляется «Администратором А», в то время как ОС хоста управляется «Администратором В». Когда два администратора одновременно эксплуатируют компоненты, то это может инициировать создание уязвимости. В этом случае CVSS считает, что изменения уже произошли. Это условие теперь отражается в новых МГ [11].

В рамках стандарта вводятся два следующих базовых понятия. Уязвимый компонент (vulnerable component) – компонент ИС, содержащий уязвимость и участвующий в процессе эксплуатации. Атакуемый компонент (impacted component) – компонент ИС, базовые характеристики безопасности которого (конфиденциальность, целостность, доступность) могут быть нарушены при успешной реализации атаки.

Как правило, уязвимый и атакуемый компоненты совпадают, но существуют классы уязвимостей, для которых это правило не работает, например: выход за пределы «песочницы» приложения; получение доступа к пользовательским данным, сохраненным в браузере, через уязвимость в Веб-приложении (XSS); выход за пределы гостевой виртуальной машины и др.

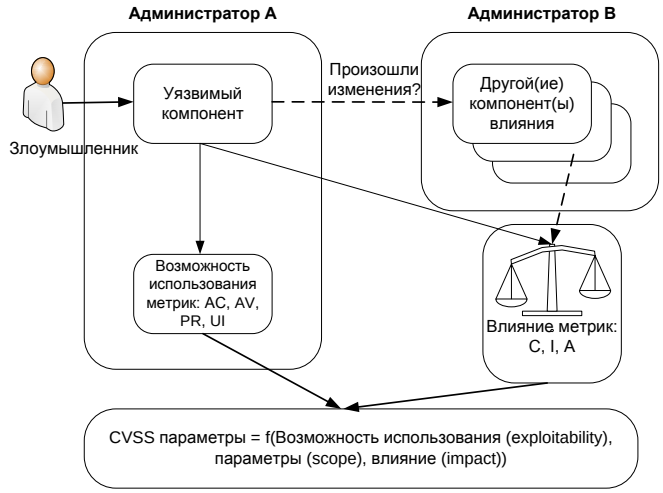


Рис. 6. Изменения в CVSS v3.0

В этой версии метрики эксплуатируемости рассчитываются для уязвимого компонента, а метрики воздействия для атакуемого. Версия CVSS v2 не позволяла отображать ситуацию, при которой уязвимый компонент и атакуемый различаются [3, 11].

В CVSS v3.0 вектор доступа (Access Vector в v2.0) был переименован в вектор атаки, но как и ранее, отражает «удаленность» злоумышленника по отношению к уязвимым компонентам. Другими словами, чем более отдаленным злоумышленник является относительно уязвимого компонента (с точки зрения логической и физической удаленности сети), тем больше будет базовая оценка. Кроме того, этот показатель различает локальные атаки, которые требуют локального доступа к системе (например, атака на прикладное приложение) и физические, которые требуют физического доступа к платформе для использования уязвимости (например, с FireWire, USB или jailbreaking атака) [10]. Изменения коснулись понятия значения показателя «Local», которое ранее описывало любые действия не затрагивающие сеть. В новом стандарте вводится следующее деление значений этого показателя. Local – для эксплуатации атакующему требуется локальная сессия или определенные действия со стороны легитимного пользователя. Physical – атакующему требуется физический доступ к уязвимой подсистеме [3].

Также изменения коснулись и показателя **AC** т.е. сложность эксплуатации уязвимости, представляющего собой качественную оценку сложности проведения атаки. Чем больше условий должно быть соблюдено для эксплуатации уязвимости – тем выше сложность [3]. Здесь были объединены два значения показателя «Low» и «Medium». Таким образом, сложность доступа была представлена в двух параметрах – сложность атаки и взаимодействие пользователя [11]. Понятие «сложность» само по себе субъективное, поэтому данный параметр, всегда трактовался экспертами по-разному. Например, для уязвимостей, позволяющих реализовать атаку «Человек посередине» (активная атака [10]) в базе NVD можно встретить различные варианты оценки **AC**. Теперь, для облегчения толкования данного параметра предлагаются только две ступени сложности «High» и «Low», а также более четко прописаны критерии отнесения к ним уязвимостей. В частности, уязвимость, позволяющую реализовать активную атаку, предписано относить к значению показателя «High». Факторы, учитываемые в CVSS v2 параметром **AC**, в новом стандарте раскрывается двумя показателями – Attack Complexity и User Interaction [3].

В CVSS v3.0 появился новый показатель «необходимые привилегии» (Privileges Required) заменяющий показатель «аутентификации» в v2.0 (аутентификация/требуемый уровень привилегий – требуется ли аутентификация для проведения атаки, и если требуется, то какая именно [3]). Необходимые привилегии, отражают уровень доступа, требуемый для успешной атаки. В частности, значения показателей «High», «Low» и «None» отражают привилегии, необходимые злоумышленнику для того, чтобы воспользоваться уязвимостью. Подход к расчету показателя, основан на количестве независимых процессов аутентификации, которые нужно пройти атакующему [3]. Все другие изменения в CVSS v3.0 отражены в таблице 2 [10].

Здесь, по аналогии с табл. 1, для каждой МГ по каждому множеству показателей приведены

наборы символьных значений и соответствующие им числовые показатели.

Таблица 2

Значения показателей оценок CVSS v3.0

МГ	Множество показателей	Наборы символьных значений показателей	Числовые значения соответствующих показателей
Базовая	**AV**	N; A; L; P	0,85; 0,62; 0,55; 0,2
	AC	H; L	0,77; 0,44
	PR	H; L; N	0,85; 0,62 (или 0,68*); 0,27 (или 0,50*)
	UI	N; R	0,85; 0,62
	S	U; C	-
	C; I; A;	N; L; H;	0; 0,22; 0,56
Временная	**E**	U; P; F; H; X	0,91; 0,94; 0,97; 1; 1
	RL	O; T; W; U; X	0,95; 0,96; 0,97; 1; 1
	RC	U; R; C; X	0,92; 0,96; 1; 1
Среды окружения	**CR; IR; AR**	L; M; H; X	0,5; 1; 1,5; 1
Модифицированная базовая	**MAV; MAC; MPR; MUI; MS; MC; MI; MA**	Имеют те же символьные и числовые значения показателей, что и соответствующие не модифицированные показатели в базовой МГ, а также «Not Defined» (по умолчанию)	

*если область действия (S)/модифицированная область действия (MS) изменяется

Кроме этого каждому символьному значению определена соответствующая им лингвистическая интерпретация – для **AV** (Attack Vector – вектор атаки): N – «Сеть»; A – «Сопряженная сеть»; L – «Локальный доступ»; P – «Физический доступ», для **AC** (Attack Complexity – сложность атаки): H – «Высокая»; L – «Средняя», для **PR** (Privileges Required – необходимые полномочия): H – «Высокие»; L – «Средние»; N – «Отсутствуют», для **C** (Confidentiality Impact – воздействие на конфиденциальность), **I** (Integrity Impact – воздействие на целостность) и **A** (Availability Impact – воздействие на доступность): H – «Высокое»; L – «Среднее»; N – «Отсутствует», для **UI** (User Interaction – взаимодействие с пользователем): N – «Отсутствует»; R – «Требуется», для **S** (Scope – область действия): U – «Без изменений»; C – «Изменена», для **E** (Exploitability – возможность использования): U – «Теоретическая (нет доказательств)»; P – «Экспериментальная»; F – «Функциональная»; H – «Высокая»; X – «Не определена», для **RL** (Remediation Level – уровень исправления): O – «Официальный патч»; T – «Временное решение»; W – «Решение на основе советов и рекомендаций»; U – «Отсутствует»; X – «Не определен», для **RC** (Report Confidence – достоверность отчета): U – «Отсутствует»; R – «Обоснована»; C – «Подтверждена»; X – «Не определена», для (Security Requirements – Требования к безопасности) **CR** (Confidentiality Requirement – требование конфиденциальности), **IR** (Integrity Requirement – требование целостности), **AR** (Availability Requirement – требование доступности): L – «Низкое»; M – «Среднее»; H – «Высокое»; X – «Не определено». Модифицированная базовая группа метрик описывается показателями **MAV** (Modified Attack Vector – модифицированный вектор атаки), **MAC** (Modified Attack Complexity – модифицированная сложность атаки), **MPR** (Modified Privileges Required – модифицированные необходимые полномочия), **MUI** (Modified User Interaction – модифицированное взаимодействие с пользователем), **MS** (Modified Scope – модифицированная область действия), **MC** (Modified Confidentiality – модифицированная конфиденциальность), **MI** (Modified Integrity – модифицированная целостность) и **MA** (Modified Availability – модифицированная доступность) (также см. рис. 6 и 7). На рис. 7 показан встроенный калькулятор показателей CVSS v3.0 в Веб-интерфейс.

Рассмотрим примеры получения значений по уязвимости CVE-2015-1098 (Apple и Work Denial of Service Vulnerability) с помощью CVSS v2.0 и CVSS v3.0 (см. табл. 3) [11].

Таблица 3

Пример вычисления CVSS

Показатель		Значение показателя		Числовое значение	
v2.0	v3.0	v2.0	v3.0	v2.0	v3.0
AV		N	L	1	0,55
AC		M	L	0,61	0,44
Au	PR	N	N	0,704	0,27
-	UI	-	R	-	0,62
-	S	-	U	-	-
C		P	H	0,275	0,56
I		P	H	0,275	0,56
A		P	H	0,275	0,56
Результаты CVSS для базовой МГ				6,8	7,8

Согласно установленным правилам каждой уязвимости присваивается CWE категория, в соответствие с которым осуществляется группирование их по определенным категориям, отображающим так называемые слабые места РИС.

Например, как показано на рис. 2, рассматриваемой уязвимости присвоена категория CWE-17, а на рис. 8 отображено описание этого кода. Согласно представленному на сайте CWE™ отчету на 07.12.2015 г. зафиксировано 1004 CWE категорий слабых мест [12].

Рис. 7. Интерфейс встроенного калькулятора CVSS v3.0
МГ: а) Базовая; б) Временная; в) Среды окружения

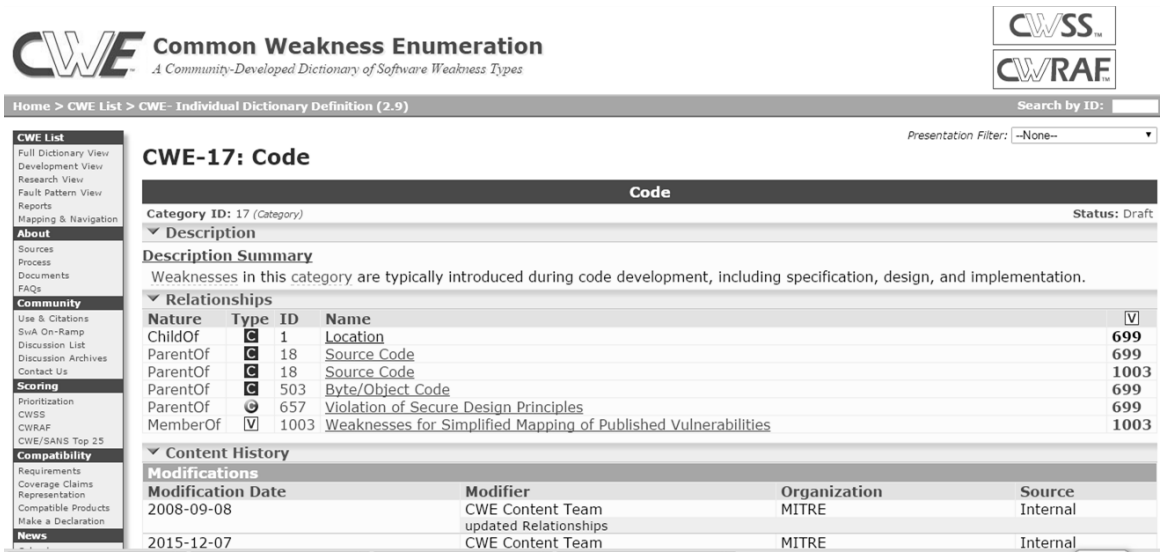


Рис. 8. Описание CWE-17 категории

Пример описания уязвимостей доступных для скачивания в БД NVD показан в таблице 4. Здесь отображены уязвимости с идентификаторами CVE-2015-0001 – «Windows Error Reporting Security Feature Bypass Vulnerability» и CVE-2015-0032 – «VBScript Memory Corruption Vulnerability». В представленной таблице каждому столбцу присвоен номер, который отражает, например, следующую информацию об уязвимостях в БД: 1 – версия базы данных; 2 – дата публикации; 3 – идентификатор угрозы; 11 – название продукта; 12 – CVE-идентификатор угрозы; 14 – дата последнего изменения; 15 – оценка CVSS (см. рис. 9); 16 – вектор доступа; 17 – сложность доступа; 18 – аутентификация; 19, 20, 21 – соответственно воздействие на конфиденциальность, целостность и доступность; 22 – источник; 23 – время появления; 24 – CWE категория; 25 – язык; 26 – тип ссылки; 30 – язык (описание по заданному адресу); 31 – резюме и др. (см. табл. 4).

Таблица 4

Пример описания уязвимостей

nvd_xml_version	pub_date	id	id2	operator	negate	name	operator3	negate4	name5	ns3:product	ns3:cve-id	ns3:published-datetime	ns3:last-modified-datetime	ns4:score	ns4:access-vector	ns4:access-complexity	ns4:authentication	ns4:confidentiality-impact	ns4:integrity-impact	ns4:availability-impact	ns4:source	ns4:generated-on-datetime	id6	ns2:lang	reference_type	ns3:source	ns3:reference	Href	ns2:lang7	ns3:summary	ns3:security-protection
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
2	09.12.2015 3:00:00	CVE-2015-0001	http://www.nist.gov/	OR	False	cpe:/o:microsoft:windows_8:-	-	-	-	cpe:/o:microsoft:windows_server_2012:r2:-:~~~~x64~~	CVE-2015-0001	2015-01-13T17:59:00.050-05:00	2015-01-14T16:50:51.080-05:00	6,9	LOCAL	MEDIUM	NONE	COMPLETE	COMPLETE	COMPLETE	http://nvd.nist.gov	2015-10-30T13:42:24.787-04:00	CWE-264	en	VENDOR_ADVISORY	MS	MS15-006	http://technet.microsoft.com/security/bulletin/MS15-006	en	*1)	-
2	09.12.2015 3:00:00	CVE-2015-0032	http://nvd.nist.gov/	AND	False	-	OR	False	cpe:/a:microsoft:vbscript:5.6	cpe:/a:microsoft:vbscript:5.7	CVE-2015-0032	2015-03-11T06:59:01.290-04:00	2015-09-10T11:58:19.313-04:00	9,3	NETWORK	MEDIUM	NONE	COMPLETE	COMPLETE	COMPLETE	http://nvd.nist.gov	2015-09-10T10:43:58.757-04:00	CWE-399	en	VENDOR_ADVISORY	MS	MS15-019	http://technet.microsoft.com/security/bulletin/MS15-019	en	*2)	-

*1) Компонент отчета об ошибках Windows (WER) в Microsoft Windows 8, Windows 8.1, Windows Server 2012 Gold, R2 и Windows RT Gold позволяет локальным пользователям обойти механизм защиты и прочитать содержимое в произвольных местах процесса-памяти за счет использования административных привилегий.

*2) vbscript.dll в Microsoft VBScript 5.6 ÷ 5.8, используемый с Internet Explorer 8 ÷ 11 и других продуктов, позволяет удаленному злоумышленнику выполнить произвольный код или вызвать отказ в обслуживании (повреждение памяти) посредством созданного Веб-сайта.

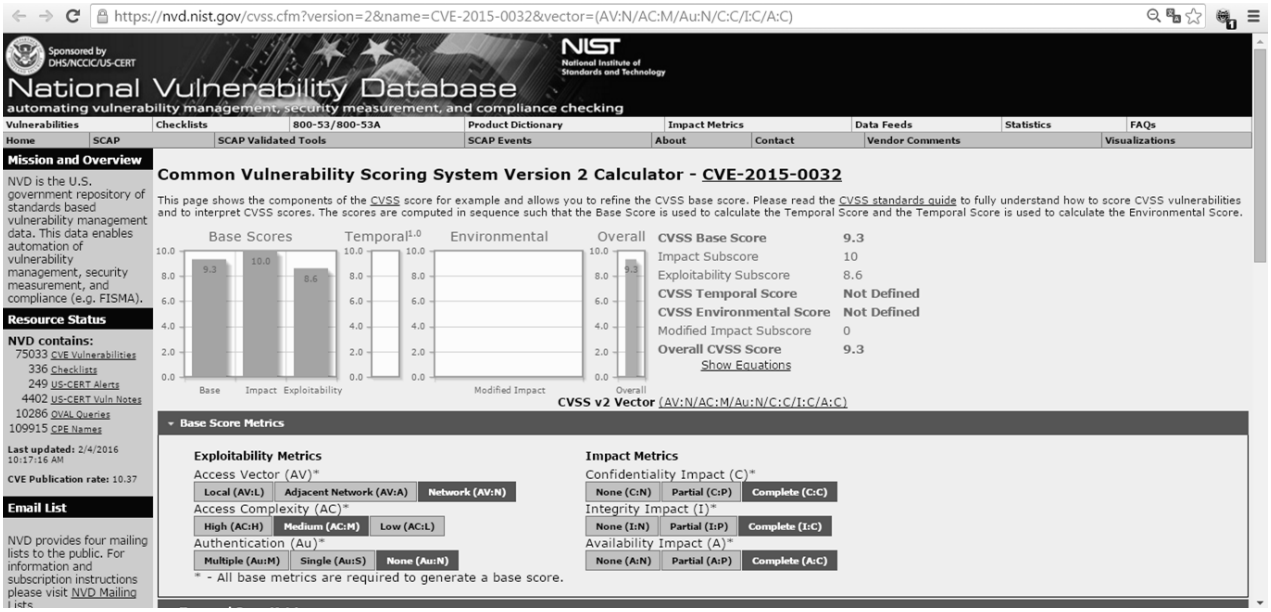


Рис. 9. Оценка CVSS для CVE-2015-0032

В ходе исследования базы NVD было установлено, что 82,77% уязвимостей принадлежат приложениям, 12,28% – ОС, а 3,59% – аппаратному обеспечению [7].

Банк данных угроз безопасности информации (БДУБИ). Банк БДУБИ разработан Федеральной службой по техническому и экспортному контролю России и Государственным научно-исследовательским испытательным институтом проблем технической ЗИ России. Банк содержит сведения об основных угрозах ИБ и уязвимостях, в первую очередь, характерных для государственных ИС и автоматизированных систем управления производственными и технологическими процессами объектов критических инфраструктур. Сведения об угрозах ИБ и уязвимостях ПО, содержащихся в БДУБИ, не являются исчерпывающими и могут быть дополнены по результатам анализа соответствующих угроз и уязвимостей в конкретной ИС с учетом особенностей ее эксплуатации. Данные, содержащиеся в БДУБИ не являются элементами иерархической классификационной системы и представляют собой обобщенный перечень основных угроз и уязвимостей ИБ (см. рис. 10) потенциально опасных для ИС. Последнее обновление БДУБИ от 11.07.16 г. содержало 186 угроз и 14395 уязвимостей [1].

Каждая угроза, вносимая в БДУБИ, описывается следующим набором параметров (рис. 10.): уникальный идентификатор УБИ (угроза безопасности информации); наименование угрозы; описание угрозы; источник угрозы (тип нарушителя и его минимально необходимый функционал (потенциал)) (см. рис. 11); объект воздействия; последствия реализации угрозы [1].

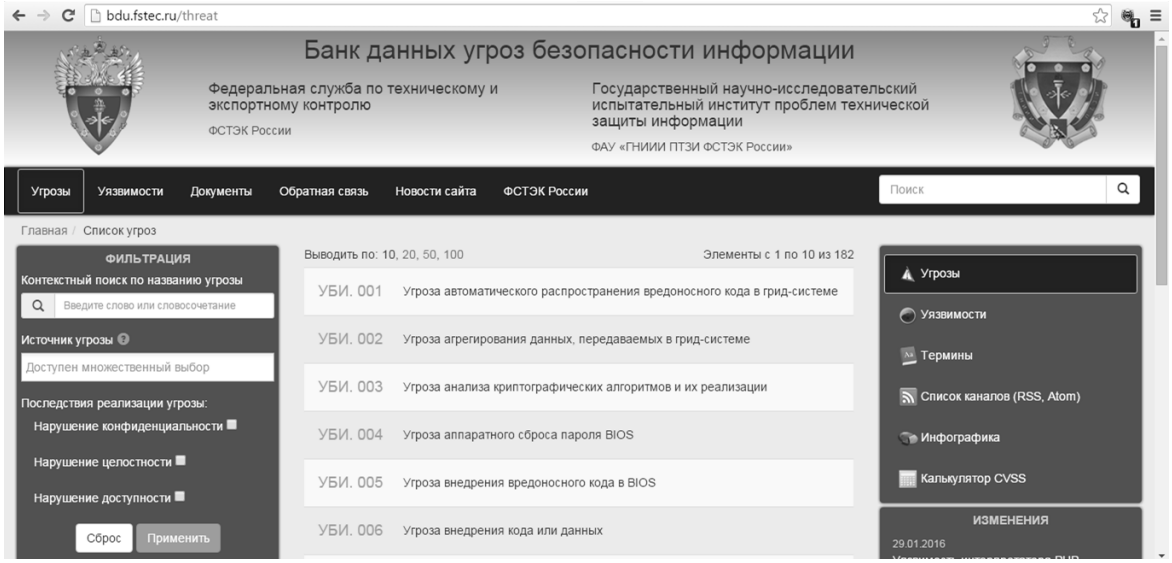


Рис. 10. Окно страницы описания угроз в БДУБИ

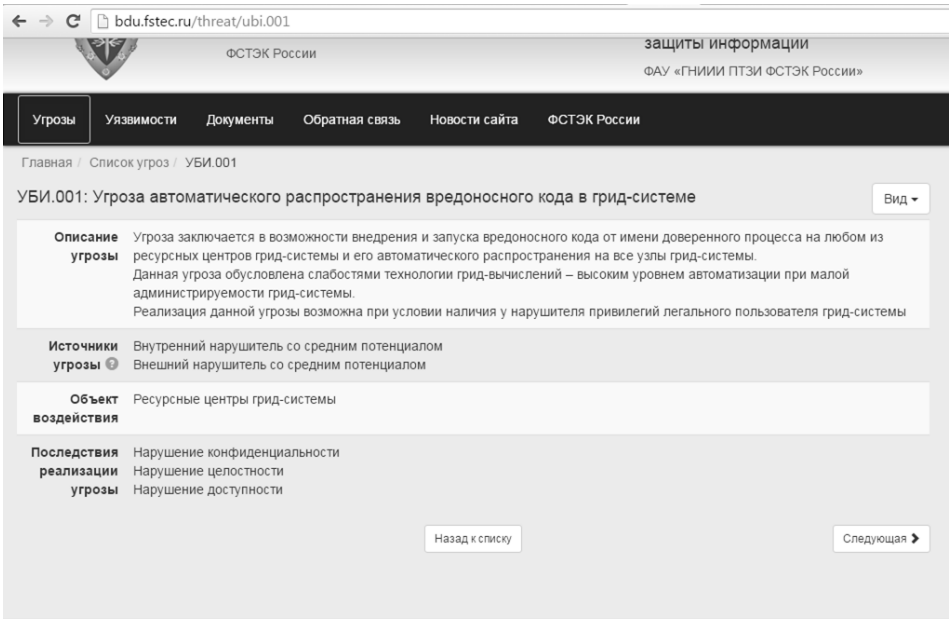


Рис. 11. Пример описания УБИ: 001

В процессе внесения в БДУБИ информации об уязвимостях используется следующий набор параметров (см. рис. 12): идентификатор (состоит из года и номера по порядку); наименование уязвимости; описание уязвимости; вендор (компания – производитель ПО в котором обнаружена уязвимость); название ПО; версия ПО; тип ПО; ОС и аппаратные платформы; тип ошибки; идентификатор типа ошибки (идентификатор, установленный в соответствии с общим перечнем ошибок CWE); класс уязвимости; дата выявления; вектор уязвимости базовой МГ (по CVSS v2.0); уровень опасности уязвимости (по CVSS v2.0); возможные меры по устранению уязвимости; статус уязвимости; наличие эксплойта; информация об устранении; ссылки на источники; идентификаторы других систем описаний уязвимостей (например, CVE); прочая информация [1] (см. таблицу 5). Также на сайте БДУБИ содержится калькулятор CVSS v2.0 (см. рис. 13), являющийся русскоязычной версией аналогичного калькулятора NVD. Здесь представлена и инфографика, на которой отображены сводные данные по разным параметрам (рис. 14).

Таблица 5

Пример отчета по уязвимостям

№п/п	1
Наименование уязвимости	Уязвимость микропрограммного обеспечения программируемого логического контроллера Schneider Electric Modicon Quantum, позволяющая злоумышленнику получить авторизованный доступ к устройству
Открытый идентификатор уязвимости	2014-00001
Идентификаторы других систем описаний уязвимости	CVE-2011-4859
Описание уязвимости	Микропрограммное обеспечение модуля 140NOE77111 контроллера Schneider Electric Modicon Quantum содержит множество пар логин: пароль, установленных по умолчанию. Это позволяет любому пользователю, имеющему доступ к устройству по протоколу FTP, получить авторизованный доступ к устройству
Название ПО	Микропрограммное обеспечение программируемого логического контроллера Schneider Electric Modicon Quantum
Версия ПО	4.6
Класс уязвимости	Уязвимость архитектуры
Наименование ОС и тип аппаратной платформы	Микропрограммное обеспечение программируемого логического контроллера Schneider Electric Modicon Quantum (4.6)
Дата выявления	17.12.2011
Базовый вектор CVSS	AV:N/AC:L/Au:N/C:C/I:C/A:C
Уровень опасности уязвимости	Критический уровень опасности (базовая оценка CVSS составляет 10)
Возможные меры по устранению	Ограничение доступа к устройству по протоколу FTP
Статус уязвимости	Подтверждена производителем
Наличие эксплойта	Существует
Информация об устранении	Информация об устранении отсутствует
Ссылки на источники	http://ics-cert.us-cert.gov/alerts/ICS-ALERT-12-020-03
Вендор ПО	Schneider Electric
Прочая информация	Язык разработки ПО – C
Описание ошибки CWE	Жесткое кодирование паролей
Тип ошибки CWE	CWE-259

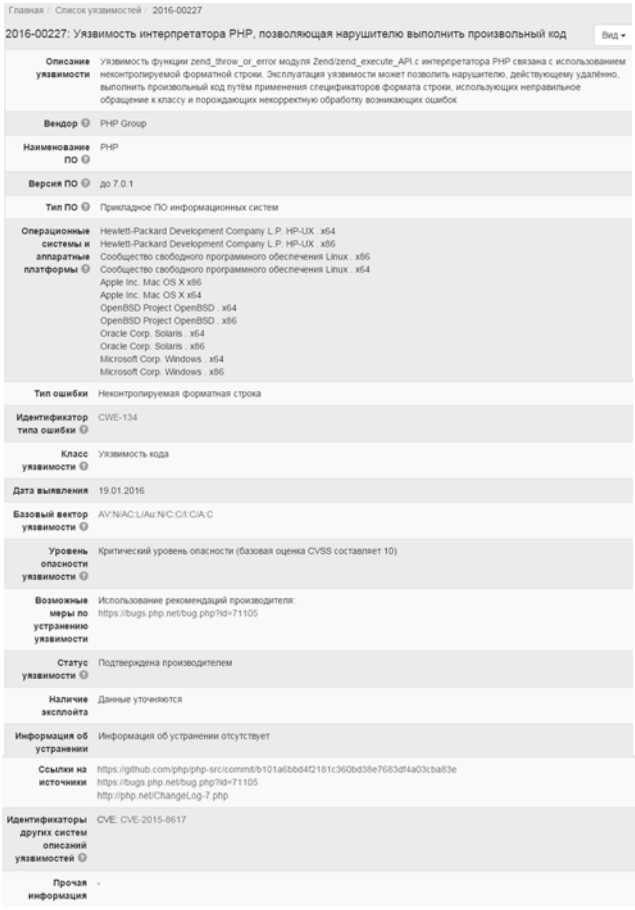


Рис. 12. Фрагмент примера описания уязвимости 2016-00227 в БДУБИ

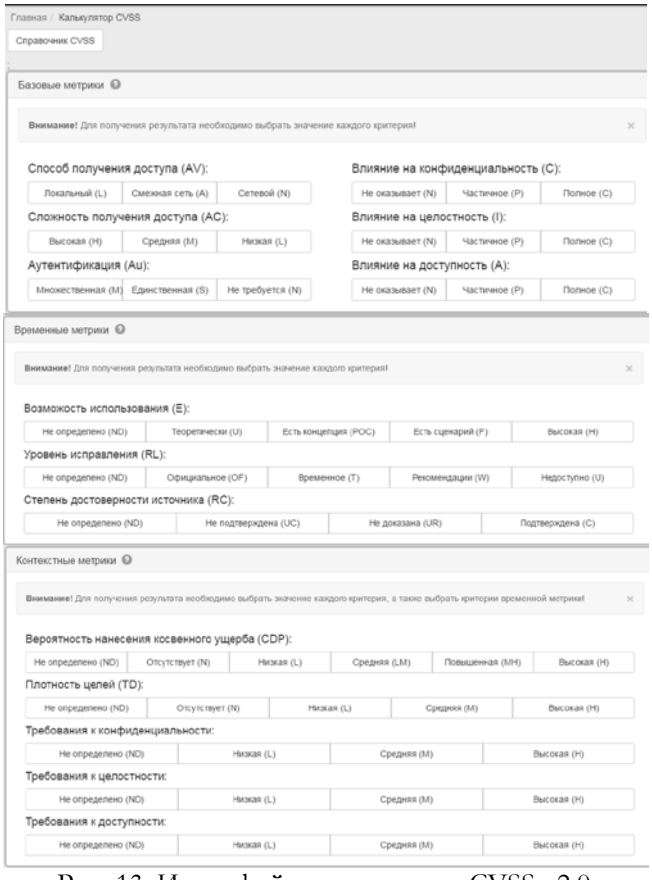


Рис. 13. Интерфейс калькулятора CVSS v2.0 на сайте БДУБИ

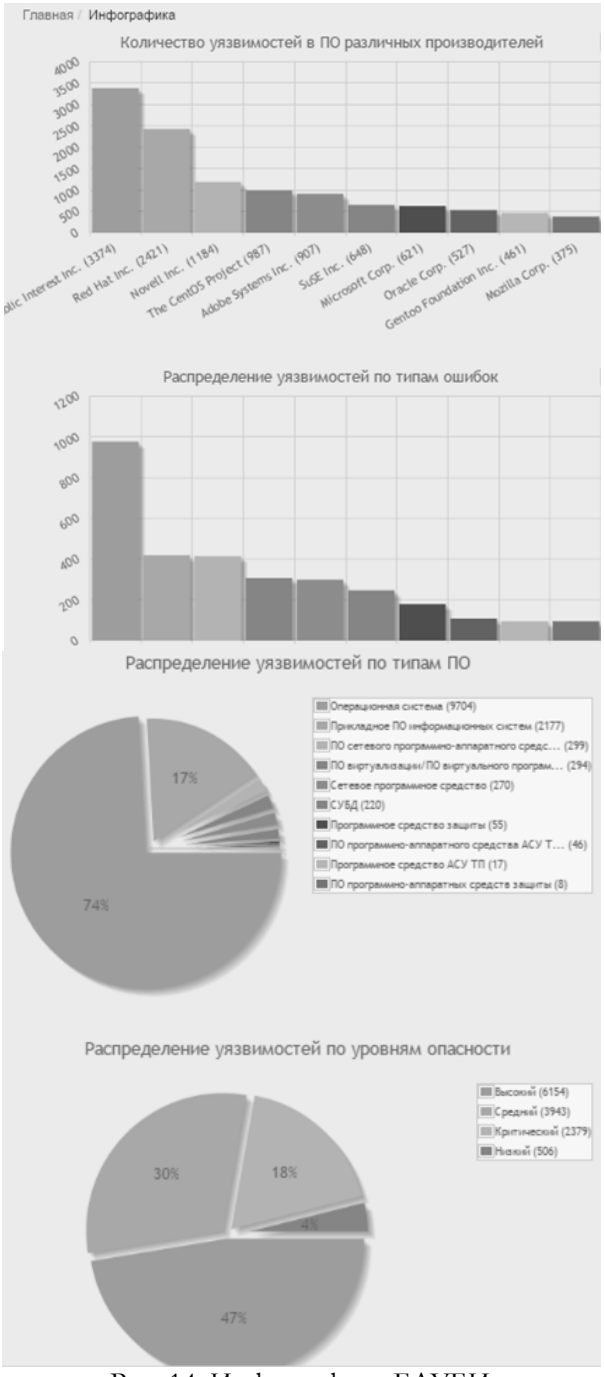


Рис. 14. Инфографика БДУБИ

Open Sourced Vulnerability Database (OSVDB). База создана OSVDB в 2002 году, как независимая и открытая БД уязвимостей для специалистов в области ИБ. Цель проекта состояла в том, чтобы обеспечить точную, детализированную и актуальную информацию об уязвимостях для систем обеспечения ИБ [7]. На 5 мая 2014 года данная база содержала 105413 уязвимостей. Веб-интерфейс OSVDB (см. рис. 15) не сильно отличается от базы NVD. Каждая уязвимость, заносимая в OSVDB, описывается следующими записями: идентификатор OSVDB; дата обнаружения; имя производителя; имя продукта; версия продукта (символьное значение), имею-

щего данную уязвимость; ссылка, указывающая на прямой адрес интернет-ресурса другой базы или базы производителя, в которой описывается данная уязвимость; решение, имеющее описание «исправления» уязвимости; метрики уязвимости, содержащие критерии оценки уязвимостей в формате CVSS v2.0 (не являются обязательными ввиду того, что поле присутствует при наличии ссылки на базу NVD) [7]. Стоит отметить, что OSVDB с 2016 года стала условно открытой БД и теперь предоставляются платные услуги по информации об уязвимостях. При этом, ее разработчики заключили сотрудничество с компанией Risk Based Security, которая продает клиентам лицензии на получение доступа к данным.

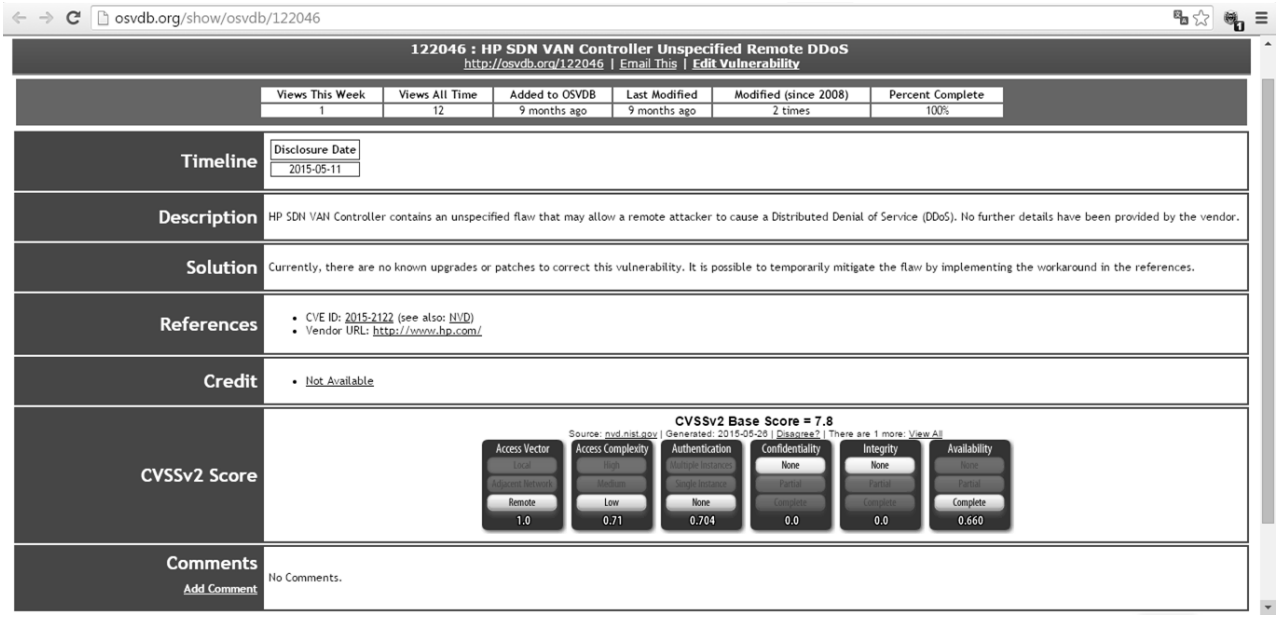


Рис. 15 Интерфейс OSVDB

База данных уязвимостей IBM X-Force. База IBM ISS (Internet Security Services) X-Force, созданная специалистами подразделения IBM Internet Security Systems X-Force, является одной из самых больших и авторитетных БД в отрасли. Она содержит свыше 30000 записей и подробный анализ каждой известной уязвимости, обнаруженной с 1994 года. Более того, специалисты подразделения X-Force сотрудничают с тысячами крупнейших в мире компаний и государственных учреждений, центрами анализа и вертикального обмена информацией (ISAC), глобальными координационными центрами и другими поставщиками решений [20]. Для доступа к БД уязвимостей необходимо пройти регистрацию на сайте IBM X-Force Exchange. После регистрации в строке поиска необходимо задать нужную информацию об уязвимости (см. рис. 16).

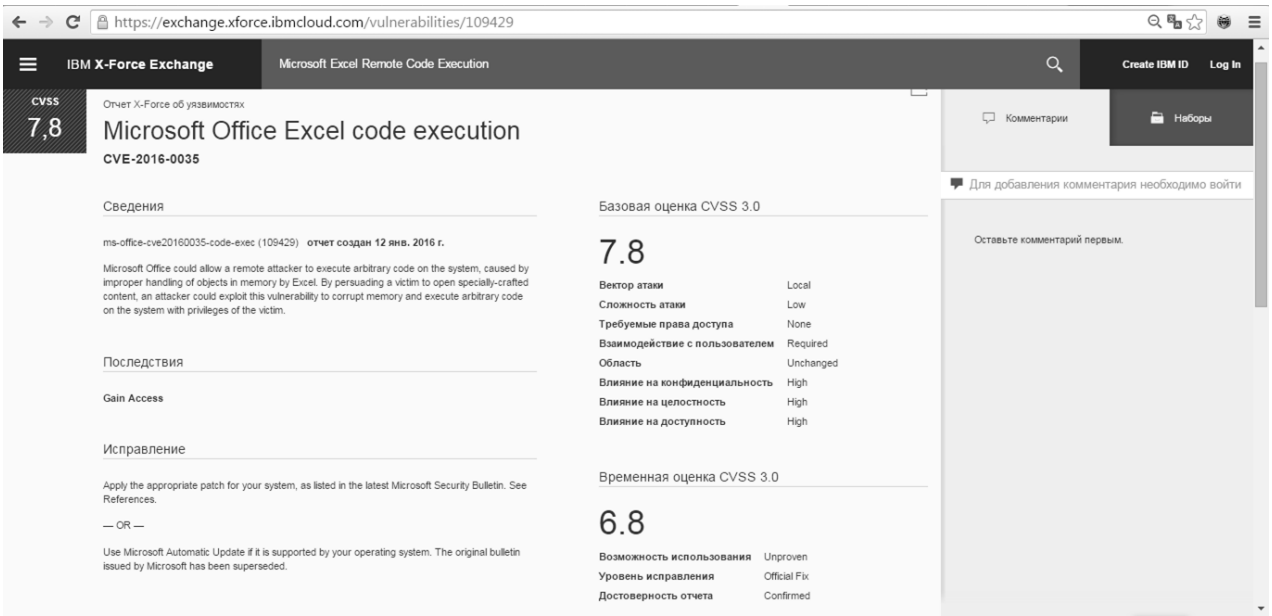


Рис. 16. Пример описания уязвимости Microsoft Excel Remote Code Execution

Как видно с описания уязвимости на рис. 16 используются, по аналогии с предыдущими базами, оценки CVSS (до 2016 года использовалась v2.0, после – v3.0), идентификатор CVE, краткое описание, дата создания отчета об уязвимости, затронутые продукты в которых есть эта уязвимость и внешние ссылки. Но в отличие от других БД здесь присутствует поле «Последствия», выражающее в формализованном виде возможный результат эксплуатации уязвимости, например, «Gain Access» (получение доступа) и «Исправление», где приведены варианты контрмер [7, 13].

База данных записей уязвимостей US-CERT. База VND (см. рис. 17) принадлежит United States Computer Emergency Readiness Team – US-CERT и разработана совместно с Office of Cybersecurity and Communications (Управление кибербезопасности и коммуникаций), Department of Homeland Security (Департамент внутренней безопасности), Software Engineering Institute (Инженерный институт ПО) и Carnegie Mellon University (Институт Карнеги-Мелоуна).

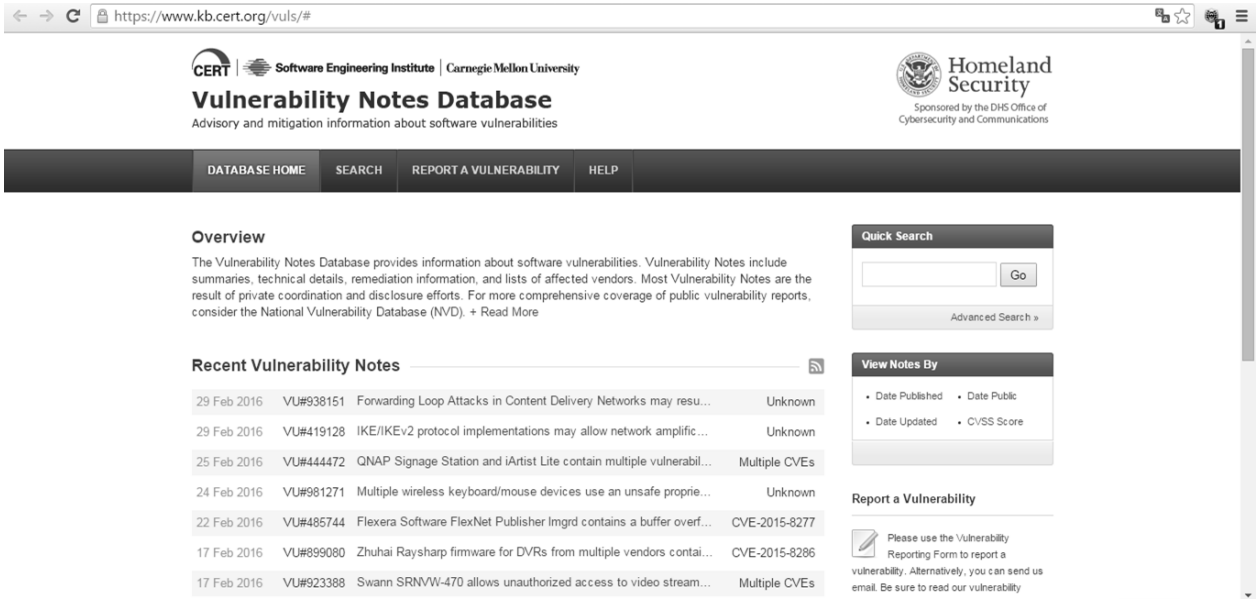
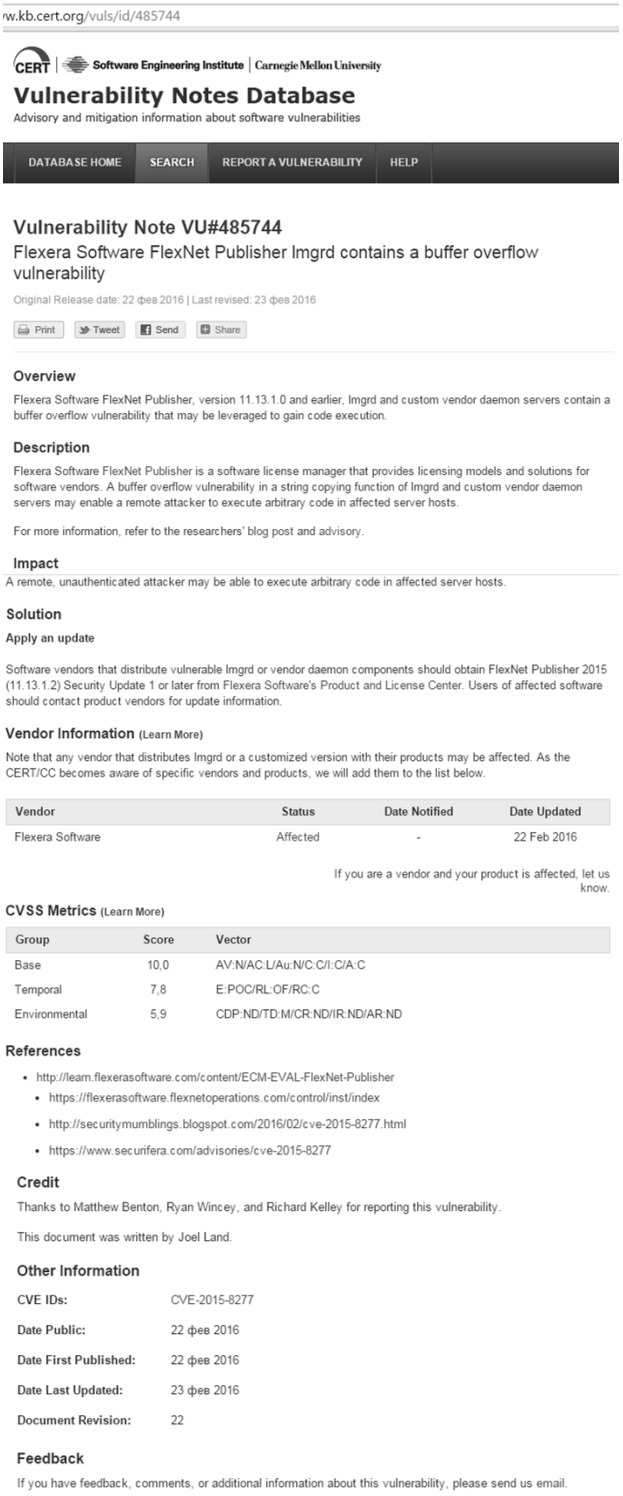


Рис. 17. Основная страница VND

Каждой уязвимости в БД присваивается свой идентификатор «VU#», как показано на рис. 18 (VU#485744). По аналогии с рассмотренными выше БД в VND присутствуют следующие основные пункты описания уязвимости: обзор; краткое описание; влияние; рекомендации об устранении; оценки CVSS; также в дополнительной информации указывается (если есть) идентификатор CVE; дата первой публикации и обновления (см. рис. 19). В отличие от остальных БД здесь уязвимости фиксируются с указанием пострадавшей стороны и информации о продавце. Так же на сайте БД VND присутствует возможность получения сводных данных оценок CVSS уязвимостей (см. рис. 19) [19].


w.kb.cert.org/vuls/id/485744

CERT | Software Engineering Institute | Carnegie Mellon University

Vulnerability Notes Database

Advisory and mitigation information about software vulnerabilities

DATABASE HOME | SEARCH | REPORT A VULNERABILITY | HELP

Vulnerability Note VU#485744

Flexera Software FlexNet Publisher lmgrd contains a buffer overflow vulnerability

Original Release date: 22 фев 2016 | Last revised: 23 фев 2016

Print | Tweet | Send | Share

Overview

Flexera Software FlexNet Publisher, version 11.13.1.0 and earlier, lmgrd and custom vendor daemon servers contain a buffer overflow vulnerability that may be leveraged to gain code execution.

Description

Flexera Software FlexNet Publisher is a software license manager that provides licensing models and solutions for software vendors. A buffer overflow vulnerability in a string copying function of lmgrd and custom vendor daemon servers may enable a remote attacker to execute arbitrary code in affected server hosts.

For more information, refer to the researchers' blog post and advisory.

Impact

A remote, unauthenticated attacker may be able to execute arbitrary code in affected server hosts.

Solution

Apply an update

Software vendors that distribute vulnerable lmgrd or vendor daemon components should obtain FlexNet Publisher 2015 (11.13.1.2) Security Update 1 or later from Flexera Software's Product and License Center. Users of affected software should contact product vendors for update information.

Vendor Information (Learn More)

Note that any vendor that distributes lmgrd or a customized version with their products may be affected. As the CERT/CC becomes aware of specific vendors and products, we will add them to the list below.

Vendor	Status	Date Notified	Date Updated
Flexera Software	Affected	-	22 Feb 2016

If you are a vendor and your product is affected, let us know.

CVSS Metrics (Learn More)

Group	Score	Vector
Base	10,0	AV:N/AC:L/Au:N/C:C/I:C/A:C
Temporal	7,8	E:POC/RL:OF/RC:C
Environmental	5,9	CDP:ND/TD:M/CR:ND/IR:ND/AR:ND

References

- http://learn.flexerasoftware.com/content/ECM-EVAL-FlexNet-Publisher
- https://flexerasoftware.flexnetoperations.com/control/inst/index
- http://securitymumblings.blogspot.com/2016/02/cve-2015-8277.html
- https://www.securifera.com/advisories/cve-2015-8277

Credit

Thanks to Matthew Benton, Ryan Wincey, and Richard Kelley for reporting this vulnerability.

This document was written by Joel Land.

Other Information

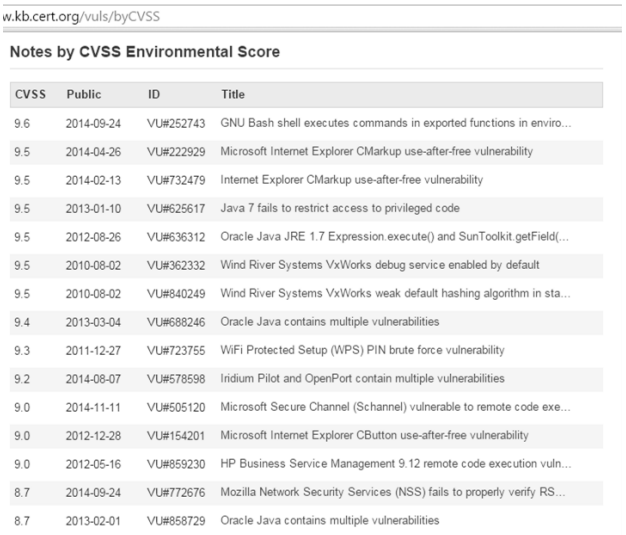
CVE IDs:	CVE-2015-8277
Date Public:	22 фев 2016
Date First Published:	22 фев 2016
Date Last Updated:	23 фев 2016
Document Revision:	22

Feedback

If you have feedback, comments, or additional information about this vulnerability, please send us email.

Рис. 18. Пример описания уязвимости

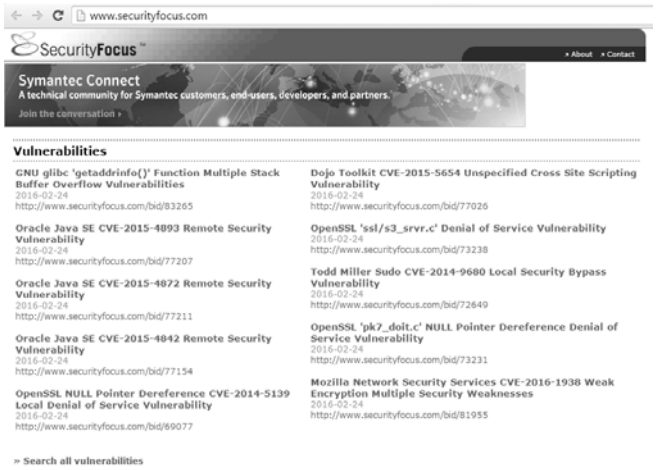
База данных уязвимостей SecurityFocus. База SecurityFocus разработана в 1999 и принадлежит компании Symantec (рис. 20) [18]. В SecurityFocus при добавлении уязвимости последней присваивается Bugtraq ID и определяется класс (рис. 21). По аналогии с другими открытыми БД уязвимость также имеет: свой идентификатор CVE; дату опубликования и обновления; информацию об удаленности или локальности; уязвимых продуктах. На сайте для каждой уязвимости дополнительно размещена информация, в виде отдельных вкладок, обсуждение (описание), информация об использовании, решение о контрмерах и рекомендации (см. рис. 21).


w.kb.cert.org/vuls/byCVSS

Notes by CVSS Environmental Score

CVSS	Public	ID	Title
9.6	2014-09-24	VU#252743	GNU Bash shell executes commands in exported functions in enviro...
9.5	2014-04-26	VU#222929	Microsoft Internet Explorer CMarkup use-after-free vulnerability
9.5	2014-02-13	VU#732479	Internet Explorer CMarkup use-after-free vulnerability
9.5	2013-01-10	VU#625617	Java 7 fails to restrict access to privileged code
9.5	2012-08-26	VU#636312	Oracle Java JRE 1.7 Expression.execute() and SunToolkit.getField(...
9.5	2010-08-02	VU#362332	Wind River Systems VxWorks debug service enabled by default
9.5	2010-08-02	VU#840249	Wind River Systems VxWorks weak default hashing algorithm in sta...
9.4	2013-03-04	VU#688246	Oracle Java contains multiple vulnerabilities
9.3	2011-12-27	VU#723755	WiFi Protected Setup (WPS) PIN brute force vulnerability
9.2	2014-08-07	VU#578598	Iridium Pilot and OpenPort contain multiple vulnerabilities
9.0	2014-11-11	VU#505120	Microsoft Secure Channel (Schannel) vulnerable to remote code exe...
9.0	2012-12-28	VU#154201	Microsoft Internet Explorer CButton use-after-free vulnerability
9.0	2012-05-16	VU#859230	HP Business Service Management 9.12 remote code execution vuln...
8.7	2014-09-24	VU#772676	Mozilla Network Security Services (NSS) fails to properly verify RS...
8.7	2013-02-01	VU#858729	Oracle Java contains multiple vulnerabilities

Рис. 19. Сводные данные оценок CVSS


www.securityfocus.com

SecurityFocus

Symantec Connect

A technical community for Symantec customers, end-users, developers, and partners.

Join the conversation ›

Vulnerabilities

GNU glibc 'getaddrinfo()' Function Multiple Stack Buffer Overflow Vulnerabilities
2016-02-24
http://www.securityfocus.com/bid/83265

Oracle Java SE CVE-2015-4893 Remote Security Vulnerability
2016-02-24
http://www.securityfocus.com/bid/77207

Oracle Java SE CVE-2015-4872 Remote Security Vulnerability
2016-02-24
http://www.securityfocus.com/bid/77211

Oracle Java SE CVE-2015-4842 Remote Security Vulnerability
2016-02-24
http://www.securityfocus.com/bid/77154

OpenSSL NULL Pointer Dereference CVE-2014-5139 Local Denial of Service Vulnerability
2016-02-24
http://www.securityfocus.com/bid/69077

Dojo Toolkit CVE-2015-5654 Unspecified Cross Site Scripting Vulnerability
2016-02-24
http://www.securityfocus.com/bid/77026

OpenSSL 'ssl/s3_srvr.c' Denial of Service Vulnerability
2016-02-24
http://www.securityfocus.com/bid/73238

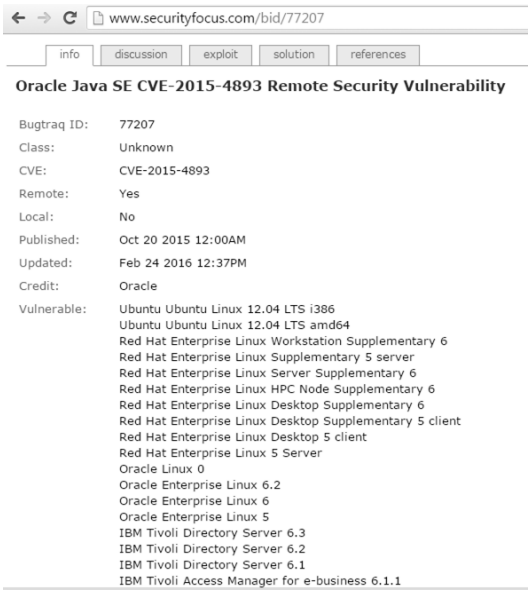
Todd Miller Sudo CVE-2014-9680 Local Security Bypass Vulnerability
2016-02-24
http://www.securityfocus.com/bid/72649

OpenSSL 'pk7_doit.c' NULL Pointer Dereference Denial of Service Vulnerability
2016-02-24
http://www.securityfocus.com/bid/73231

Mozilla Network Security Services CVE-2016-1938 Weak Encryption Multiple Security Weaknesses
2016-02-24
http://www.securityfocus.com/bid/81955

» Search all vulnerabilities

Рис. 20. Основная страница БД SecurityFocus


www.securityfocus.com/bid/77207

info | discussion | exploit | solution | references

Oracle Java SE CVE-2015-4893 Remote Security Vulnerability

Bugtraq ID:	77207
Class:	Unknown
CVE:	CVE-2015-4893
Remote:	Yes
Local:	No
Published:	Oct 20 2015 12:00AM
Updated:	Feb 24 2016 12:37PM
Credit:	Oracle
Vulnerable:	Ubuntu Ubuntu Linux 12.04 LTS i386 Ubuntu Ubuntu Linux 12.04 LTS amd64 Red Hat Enterprise Linux Workstation Supplementary 6 Red Hat Enterprise Linux Supplementary 5 server Red Hat Enterprise Linux Server Supplementary 6 Red Hat Enterprise Linux HPC Node Supplementary 6 Red Hat Enterprise Linux Desktop Supplementary 6 Red Hat Enterprise Linux Desktop Supplementary 5 client Red Hat Enterprise Linux Desktop 5 client Red Hat Enterprise Linux 5 Server Oracle Linux 0 Oracle Enterprise Linux 6.2 Oracle Enterprise Linux 6 Oracle Enterprise Linux 5 IBM Tivoli Directory Server 6.3 IBM Tivoli Directory Server 6.2 IBM Tivoli Directory Server 6.1 IBM Tivoli Access Manager for e-business 6.1.1

Рис. 21. Фрагмент окна с примером описания уязвимости Bugtraq 77270

В результате проведенного исследования представленных в работе БД можно сделать выводы, что практически каждой уязвимости вносимой в ту или иную базу присваивается идентификатор CVE и определяется оценка CVSS. Также во время исследования были определены критерии (см. таблицу 6), по которым можно реализовывать сравнение подобных БД. К таким критериям относятся наличие: оценки CVSS по v2.0 и/или v3.0; калькулятора CVSS; идентификатора CVE; CWE категории; возможности расширения; вывода критических угроз/уязвимостей; возможности интеграции; оценки риска/риск-калькулятора. Приведенные критерии могут быть полезны разработчикам систем оценивания ИБ.

Так же стоит отметить, что процедура оценивания риска не предусмотрена ни в одной из представленных БД.

Таким образом, в работе определен набор критериев для БД уязвимостей РИС по которым можно осуществить сравнительный анализ таких баз и выбрать наиболее подходящие для построения различных средств оценивания состояния ИБ, например, систем оценивания рисков или риск-калькуляторов.

Таблица 6

Сводные данные исследования БД уязвимостей

БД	Критерии									
	Оценка риска/ риск-калькулятор	Версии CVSS		Калькулятор CVSS		CVE идентификатор	CWE категория	Возможность расширения	Вывод критических угроз/ уязвимостей	Возможность интеграции
		v2.0	v3.0	v2.0	v3.0					
NVD	-	+	+	+	+	+	+	+	-	+
БДУБИ	-	+	-	+	-	+	+	+	-	-
OSVDB	-	+	-	-	-	+	-	-	-	+
IBM X-Force	-	+	+	-	-	+	+	+	-	+
VND	-	+	+	-	-	+	+	+	+	+
Security Focus	-	-	-	-	-	+	-	+	-	+

ЛИТЕРАТУРА

[1]. Банк данных угроз безопасности информации [Электронный ресурс] / Федеральной службой по техническому и экспортному контролю России – Москва, 2016 – Режим доступа: World Wide Web. – URL: http://bdu.fstec.ru/.

[2]. Белобородов А.Ю. Применение баз данных уязвимостей в задачах исследования безопасности программных средств / А.Ю. Белобородов, А.В. Горбенко // Вісник Харківського національного технічного університету сільського господарства імені Петра Василенка. – 2015. – Вип. 165. – С. 83-85.

[3]. Компания Positive Technologies: Оценка уязвимостей CVSS 3.0 [Электронный ресурс] / HABRAHABR Сообщество IT-специалистов – Москва, 2016 – Режим доступа: World Wide Web. – URL: https://habrahabr.ru/ company/ pt/blog / 266485/.

[4]. Малюк А.А. Один из подходов к оценке рисков информационной безопасности в облачных средах / А.А. Малюк, А.В. Царегородцев, Е.В. Макаренко // Безопасность информационных технологий. – 2014. – № 4. – С. 68-74.

[5]. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі, НД ТЗІ 3.7-003-05, Державна служба спеціального зв'язку та захисту інформації України, 2005, 11 с.

[6]. Урзов А.Ю. Модель защищенной информационной системы на основе автоматизации процессов управления и мониторинга угроз безопасности / А.Ю. Урзов, С.К. Варлатая // Доклады ТУСУРа. – 2013. – № 2 (28). – С. 142-146.

[7]. Федорченко А.В. Исследование открытых баз уязвимостей и оценка возможности их применения в системах анализа защищенности компьютерных сетей / А. В. Федорченко, А. А. Чечулин, И.В. Котенко // Информационно-управляющие системы. – 2014. - №5 (72). – С. 72-79.

[8]. Федорченко А.В. Построение интегрированной базы уязвимостей / А.В. Федорченко, А.А. Чечулин, И.В. Котенко // Известия высших учебных заведений. Приборостроение. 2014. – Т.57. – №11. – С. 62-67.

[9]. Харченко В.С. Формирование подмножеств уязвимостей доступности коммерческих Вебсервисов / В.С. Харченко, Алаа Мохаммед Абдул-Хади, Ю.Л. Поночовный // Системи обробки інформації. – 2013. – випуск 7 (114). – С. 112-115.

[10]. A Complete Guide to the Common Vulnerability Scoring System. Version 2.0 [Electronic resource] / Forum of Incident Response and Security Teams – Morrisville, 2016 – Access mode: World Wide Web. – URL: http://www.first.org/cvss/v2/guide.

[11]. Common Vulnerability Scoring System v3.0: User Guide [Electronic resource] / Forum of Incident

Response and Security Teams – Morrisville, 2016 – Access mode: World Wide Web. – URL: http://www.first.org/cvss/user-guide.
[12]. CWE™ International in scope and free for public use [Electronic resource] / MITRE – Bedford, 2016 – Access mode: World Wide Web. – URL: http://cwe.mitre.org/index.html.
[13]. IBM X-Force Exchange [Electronic resource] / IBM Corporation – New York, 2016 – Access mode: World Wide Web. – URL: https:// exchange. xforce. ibmcloud.com/ vulnerabilities/109429.
[14]. Information technology. Security techniques. Information security management systems. Requirements: ISO/IEC 27001:2013, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), 2013, 34 p.
[15]. National Vulnerability Database [Electronic resource] / National Institute of Standards and Technology – Gaithersburg, 2016 – Access mode: World Wide Web. – URL: https://nvd.nist.gov/home.cfm.
[16]. Open Sourced Vulnerability Database [Electronic resource] / Open Security Foundation – Lafayette, 2016 – Access mode: World Wide Web. – URL: https:// http://osvdb.org/
[17]. Security and Privacy Controls for Federal Information Systems and Organizations [Rebecca M. Blank, Patrick D. Gallagher] : National Institute of Standards and Technology Special Publication 800-53r4 – Falls Church : Natl. Inst. Stand. Technol, 2013. – 462 p.
[18]. Vulnerabilities [Electronic resource] / SecurityFocus - Mountain View, 2016 - Access mode: World Wide Web. – URL: http://www.securityfocus.com/-53r4 – Falls Church : Natl. Inst. Stand. Technol, 2013. – 462 p.
[19]. Vulnerability Notes Database [Electronic resource] / United States Computer Emergency Readiness Team - Murray Lane, 2016 - Access mode: World Wide Web. – URL: https://www.kb.cert.org/vuls/#
[20]. X-Force – команда исследователей и разработчиков IBM Internet Security Systems (ISS) [Электронный ресурс] / IBM Corporation – New York, 2016 – Режим доступа: World Wide Web. – URL: https://www.ibm.com/ru/services/iss/research.html

REFERENCES

[1]. Data Bank information security threats [Electronic resource] / by the Federal Service for Technical and Export Control of Russia, Moscow, 2016, Access mode: World Wide Web.: URL: http://bdu.fstec.ru/.
[2]. Beloborodov Yu., Gorbenko A. Primeneniye baz dannykh uyazvimostey v zadachakh issledovaniya bezopasnosti programmnykh sredstv, Vísnik Kharkívs'kogo natsíonal'nogo tekhníchnogo uníversitetu síl's'kogo gospodarstva ímení Petra Vasilenka, 2015., Vip. 165, p. 83-85.
[3]. Company Positive Technologies: Otsenka uyazvimostey CVSS 3.0 [Electronic resource] / HABRAHABR Community IT-specialists, Moscow, 2016, Access mode: World Wide Web. – URL: https://habrahabr.ru/company/pt/blog/266485/.
[4]. Malyuk A., Tsaregorodtsev A., Makarenko Ye. Odin iz podkhodov k otsenke riskov informatsionnoy bezopasnosti v oblachnykh sredakh, Bezopasnost' informatsionnykh tekhnologiy, 2014, № 4, p. 68-74.
[5]. Poryadok provedennya robít íz stvorennya kompleksnoí sistemi zakhistu ínformatsíí v ínformatsíyno-telekomunікatsíyníy sistemí, ND TZÍ 3.7-003-05, Derzhavna sluzhba spetsíal'nogo zv'yazku ta zakhistu ínformatsíí Ukraíni, 2005, 11 p.
[6]. Urzov Yu., Varlataya S. Model secure information systems based on automation of management processes and monitoring of security threats, Reports TUSUR., 2013, № 2 (28), p. 142-146.
[7]. Fedorchenko A., Chechulin A., Kotenko I. Issledovaniye otkrytykh baz uyazvimostey i otsenka vozmozhnosti ikh primeneniya v sistemakh analiza zashchishchennosti komp'yuternykh setey, Informatsionno-upravlyayushchiye sistemy, 2014, №5 (72), p. 72-79.
[8]. Fedorchenko A., Chechulin A., Kotenko I. Postroyeniye integrirovannoy bazy uyazvimostey, Izvestiya vysshikh uchebnykh zavedeniy. Priborostroyeniye, 2014, T.57, №11, p. 62-67.
[9]. Kharchenko V., Alaa Mokhammed Abdul-Khadi, Ponochovnyy YU. Formirovaniye podmnozhestv uyazvimostey dostupnosti kommercheskikh Veb-servisov, Sistemi obrobki ínformatsíí, 2013, vipusk 7 (114), p. 112-115.
[10]. A Complete Guide to the Common Vulnerability Scoring System. Version 2.0 [Electronic resource] / Forum of Incident Response and Security Teams – Morrisville, 2016 – Access mode: World Wide Web. – URL: http://www.first.org/cvss/v2/guide.
[11]. Common Vulnerability Scoring System v3.0: User Guide [Electronic resource] / Forum of Incident Response and Security Teams – Morrisville, 2016 – Access mode: World Wide Web. – URL: http://www.first.org/cvss/user-guide.
[12]. CWE™ International in scope and free for public use [Electronic resource] / MITRE – Bedford, 2016 – Access mode: World Wide Web. – URL: http://cwe.mitre.org/index.html.
[13]. IBM X-Force Exchange [Electronic resource] / IBM Corporation – New York, 2016 – Access mode: World Wide Web. – URL: https:// exchange.xforce.ibmcloud.com/ vulnerabilities /109429
[14]. Information technology. Security techniques. Information security management systems. Requirements: ISO/IEC 27001:2013, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), 2013, 34 p.
[15]. National Vulnerability Database [Electronic resource] / National Institute of Standards and Technology – Gaithersburg, 2016 – Access mode: World Wide Web. – URL: https://nvd.nist.gov/home.cfm.

[16]. Open Sourced Vulnerability Database [Electronic resource] / Open Security Foundation – Lafayette, 2016 – Access mode: World Wide Web. – URL: https:// http://osvdb.org/
[17]. Security and Privacy Controls for Federal Information Systems and Organizations [Rebecca M. Blank, Patrick D. Gallagher] : National Institute of Standards and Technology Special Publication 800-53r4 – Falls Church : Natl. Inst. Stand. Technol, 2013. – 462 p.
[18]. Vulnerabilities [Electronic resource] / SecurityFocus - Mountain View, 2016 - Access mode: World Wide Web. – URL: http://www.securityfocus.com/-53r4 – Falls Church : Natl. Inst. Stand. Technol, 2013. – 462 p.
[19]. Vulnerability Notes Database [Electronic resource] / United States Computer Emergency Readiness Team - Murray Lane, 2016 - Access mode: World Wide Web. – URL: https://www.kb.cert.org/vuls/#.
[20]. X-Force – the research and development command IBM Internet Security Systems (ISS) [Electronic resource] / IBM Corporation – New York, 2016 – Access mode: World Wide Web. – URL: https://www.ibm.com/ru/services/iss/research.html

ДОСЛІДЖЕННЯ БАЗ ДАНИХ УРАЗЛИВОСТЕЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Існуючі загальнодоступні бази даних уразливостей зберігають в собі різні дані про відомі вразливості ресурсів інформаційних систем. Описи уразливостей містять як передумови, так і оцінки, що характеризують результат реалізації атак, які експлуатують ці уразливості. Часто перед фахівцями, які займаються дослідженням стану безпеки інформаційних систем, виникає питання про вибір відповідних баз даних. Ці бази, відповідно визначених критеріїв, можуть ефективно використовуватися для побудови різних систем оцінювання стану інформаційної безпеки, наприклад, систем оцінювання ризиків. У зв'язку з цим досліджено широкий спектр відповідних баз даних і визначені критерії, за якими можна здійснити їх порівняльний аналіз. Це дасть можливість підвищити ефективність вирішення завдань оцінювання стану безпеки ресурсів інформаційних систем.

Ключові слова: база даних уразливостей, оцінювання уразливостей, ресурси інформаційних систем, інформаційна безпека, аналіз баз даних уразливостей.

RESEARCH of INFORMATION SECURITY DATABASE VULNERABILITIES

Existing public database vulnerabilities store a variety of data about known vulnerabilities of information systems resources. Descriptions of vulnerabilities contain both precondition and assessment, describing the result of the realization of attacks that exploit these vulnerabilities. Often experts involved in research for the condition of information systems security, think of a choice of relevant databases. These bases, on certain criteria, can effectively be used to build a variety of assessment systems of the information security state, such as risk assessment systems. In this connection, it was examined a wide range of relevant databases and defined the criteria what enables to carry out a comparative analysis. This will provide an opportunity to enhance the effectiveness of rating the security state of information systems resources.

Keywords: database vulnerabilities, vulnerabilities assessment, information system, information security, analysis of database vulnerabilities.

Корченко Александр Григорьевич, доктор технических наук, профессор, лауреат Государственной премии Украины в области науки и техники, заведующий кафедрой безопасности информационных технологий Национального авиационного университета, старший научный сотрудник Национальной академии СБ Украины.
E-mail: icaocentre@nau.edu.ua

Корченко Олександр Григорович, доктор технічних наук, професор, лауреат Державної премії України в галузі науки і техніки, завідувач кафедри безпеки інформаційних технологій Національного авіаційного університету, старший науковий співробітник Національної академії СБ України.

Korchenko Oleksandr, Dr Eng (Information security), professor, laureate of the State Prize of Ukraine in Science and Technology, Head of IT-Security Academic Department, National Aviation University, Senior Researcher of the National Academy of SS of Ukraine.

Казмирчук Светлана Владимировна, кандидат технических наук, доцент, доцент кафедры безопасности информационных технологий Национального авиационного университета.
E-mail: sv.kazmirchuk@gmail.com

Казмірчук Світлана Володимирівна, кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.

Kazmirchuk Svitlana, PhD in Eng., Associate Professor of IT-Security Academic Department, National Aviation University.

Арджомандифард Алиреза, аспирант кафедры безопасности информационных технологий Национального авиационного университета.
E-mail: alireza1987@ukr.net.

Арджомандіфард Аліреза, аспірант кафедри безпеки інформаційних технологій Національного авіаційного університету.

Ardzhomandifard Alireza, postgraduate student of IT-Security Academic Department, National Aviation University.

Панивко Татьяна Валерьевна, аспирант кафедры безопасности информационных технологий Национального авиационного университета.
E-mail: pani.tasha@gmail.com.

Панівко Тетяна Валеріївна, аспірант кафедри безпеки інформаційних технологій Національного авіаційного університету.

Panivko Tetyana, postgraduate student of IT-Security Academic Department, National Aviation University.