УДК 004.056
DOI: 10.31673/2409-7292.2021.040613

Скрябін Ф.К., Вишнівський В.В.

УПРАВЛІННЯ ВИПРАВЛЕННЯМИ ТА ОНОВЛЕННЯМИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА БАЗІ РІШЕННЯ HCL BIGFIX PATCH

В роботі досліджено методи та засоби управління оновленнями та виправленнями програмного забезпечення на прикладі рішення HCL BigFix Patch. Визначено призначення, основні функції та склад програмного комплексу HCL BigFix Patch. На основі досліджень проведених в роботі розроблено варіант технології управління оновленнями та виправленнями програмного забезпечення на прикладі рішення HCL BigFix Patch. Розроблено рекомендації щодо застосування технології управління оновленнями та виправленнями програмного забезпечення корпоративної інформаційної системи.

Ключові слова: корпоративна інформаційна система, вразливості програмного забезпечення, кібербезпека, управління оновленнями та виправленнями.

Вступ

Сучасні підходи до вирішення проблеми виправлення та оновлення ПЗ корпоративної інформаційної системи базуються на централізованому управлінні виправленнями, яке відіграє ключову роль в забезпеченні її кібербезпеки [1]. Стандарт NIST [2] визначає управління виправленнями як процес виявлення, отримання, установки і перевірки виправлень для продуктів і систем. Оскільки програмне забезпечення та, відповідно, загрози для цього програмного забезпечення постійно розвиваються, фахівцям із кібербезпеки потрібні ефективні методи оцінювання, розгортання та управління постійним потоком виправлень та оновлень для безлічі операційних систем і додатків в їх гетерогенних середовищах. Для системних адміністраторів, відповідальних за потенційно тисячі кінцевих точок, що працюють під управлінням різних операційних систем і ПЗ, управління виправленнями може легко перевантажити і без того напружені бюджети і персонал [3].

Рішення HCL BigFix Patch задовольняє потреби в швидкому розгортанні і високій доступності шляхом автоматизації процесу установки виправлень, яке адмініструється з єдиної консолі. Рішення HCL BigFix Patch надає компаніям великі можливості щодо доставки виправлень для ОС Microsoft Windows, UNIX, Linux і Apple Macintosh; інших додатків від постачальників, включаючи Adobe, Mozilla, Apple і Java; до кінцевих точок, незалежно від їх місця розташування, типу підключення або статусу. Кінцеві точки можуть включати в себе сервери, ноутбуки, настільні комп'ютери та спеціалізоване обладнання, таке як POS термінали, банкомати та кіоски самообслуговування. Крім того, віртуальні машини повинні також бути виправлені, щоб віртуальні і хмарні середовища мали той же рівень кібербезпеки, що і фізичні системи [4].

BigFix Patch працює на загальній платформі BigFix [4]. BigFix є багаторівневою технологічною платформою, яка виступає в якості основної частини глобальної IT-інфраструктури. Платформа BigFix являє собою динамічну, керовану контентом систему обміну повідомленнями та управління, яка розподіляє роботу з управління IT-інфраструктурою між самими керованими пристроями, агентами.

Таким чином, технологія управління виправленнями та оновленнями програмного забезпечення є важливою складовою забезпечення кібербезпеки інформаційних систем підприємства. Централізоване управління виправленнями та оновленнями програмного забезпечення спрощує роботу адміністраторів безпеки, підвищує якість даного процесу та скорочує час їх втілення в активи, що безпосередньо впливає на кількість вразливостей, які мають місце в корпоративній інформаційній системі [5]. Вищесказане визначає актуальність теми дослідження щодо технології управління виправленнями та оновленнями програмного забезпечення корпоративної інформаційної системи на прикладі рішення HCL BigFix Patch.

Мета роботи: розробити варіант технології управління оновленнями та виправленнями програмного забезпечення корпоративної інформаційної системи на прикладі рішення HCL BigFix Patch.

Аналіз проблеми наявності вразливостей та визначення необхідності впровадження технології управління оновленнями та виправленнями програмного забезпечення

Сама система оновлень та виправлень може бути вразливою та джерелом розповсюдження шкідливого програмного забезпечення. Прикладом є кібератака з використанням вразливості вітчизняної компанії-розробника "M.E.Doc".

27.06.2017 в 10 годин 30 хвилин українські державні структури і приватні компанії через вразливості ПЗ «M.E.doc.» (програмне забезпечення для звітності та документообігу) масово потрапили під удар вірусу-шифрувальника (ransomware) Diskcoder.C (ExPetr, PetrWrap, Petya, NotPetya). Експертами було встановлено, що ураження інформаційних систем українських компаній відбулось, через оновлення програмного забезпечення, призначеного для звітності та документообігу – «M.E.Doc» [6]. За отриманими даними (підтверджено правоохоронними органами іноземних держав та міжнародними компаніями, що здійснюють діяльність у сфері інформаційної безпеки), зловмисники здійснили несанкціоноване втручання в роботу одного з персональних комп'ютерів компанії-розробника вказаного програмного забезпечення ТОВ «Інтелект-Сервіс» [6].

Отримавши доступ до вихідних кодів, вони в одне із оновлень програми вбудували бекдор (backdoor) – програму, яка встановлювала на комп'ютерах користувачів «M.E.Doc» несанкціонований віддалений доступ. Таке оновлення програмного забезпечення ймовірно відбулося ще 15.05.2017 року. Представники компанії-розробника "M.E.Doc" були проінформовані про наявність вразливостей в їх системах антивірусними компаніями, але це було проігноровано. Компанія-виробник заперечила проблеми з безпекою і назвала це «збігом» [6]. Разом з тим було з'ясовано, що виявлений бекдор за функціоналом має можливість збирати коди ЄДРПОУ уражених компаній та відправляти їх на віддалений сервер, завантажувати файли, збирати інформацію про операційну систему та ідентифікаційні дані користувачів [6, 7].

Після спрацювання бекдору, атакери компрометували облікові записи користувачів, з метою отримання повного доступу до мережі. Далі отримували доступ до мережевого обладнання з метою виведення його з ладу. За допомогою IP KVM здійснювали завантаження власної операційної системи на базі TINY Linux [6]. Зловмисники, з метою приховування вдалої кібероперації щодо масового ураження комп'ютерів та несанкціонованого збору з них інформації, тим же самим способом, через останні оновлення ПЗ «M.E.Doc» розповсюдили модифікований ransomware Petya [6]. Видалення та шифрування файлів операційних систем, було вчинено з метою видалення слідів попередньої злочинної діяльності (бекдору), та відвернення уваги шляхом імітації вимагання грошових коштів від потерпілих [6].

Слідством опрацьовувалась версія, що справжніми цілями були стратегічно-важливі для держави компанії, атаки на які, могли дестабілізувати ситуацію в країні [6]. Комплексний аналіз обставин зараження дозволяє припустити, що особи, які організували напади з використанням WannaCry, можуть бути причетні до вірусної атаки на українські державні структури і приватні компанії 27 червня 2017 року, оскільки способи розповсюдження та загальна дія подібні вірусу-шифрувальнику (ransomware) Diskcoder.C (ExPetr, PetrWrap, Petya, NotPetya) [6]. Наведені вище приклади та відповідні існуючі проблеми підтримання програмного забезпечення корпоративних інформаційних систем в актуальному та безпечному стані визначає актуальність та необхідність впровадження технології управління оновленнями та виправленнями програмного забезпечення (Patch Management).

Варіант технології управління оновленнями та виправленнями програмного забезпечення на прикладі рішення Hcl Bigfix Patch

Розглянемо дії оператора щодо управління оновленнями та виправленнями програмного забезпечення корпоративної інформаційної системи за допомогою програми Patch Management на встановленому сервері BigFix. Всі кроки виконуються оператором з консолі BigFix. Цей порядок можна застосувати до операційних систем Windows. Оператор

можете виконати ті ж процедури, щоб включити і застосувати виправлення також в інших операційних системах. Сценарій розділений на дві частини [8]: налаштування управління виправленнями для виправлень Windows; застосування патча Windows.

Налаштування управління виправленнями для виправлень Windows

Після установки продукт BigFix автоматично налаштовується для підписки на певні сайти управління і обслуговування. Таким чином, контент з цих сайтів автоматично перетікає в мережу підприємства і оцінюється на предмет відповідності на всіх комп'ютерах, на яких працює клієнт BigFix. На доступних сайтах (рис. 1) увимкнути *Enable* рядом з *BES Asset Discovery, Patches for Windows (English), Patching support* та *Updates for Windows Applications* для дозволу завантаження контенту з сайту Patch Management (рис. 1).

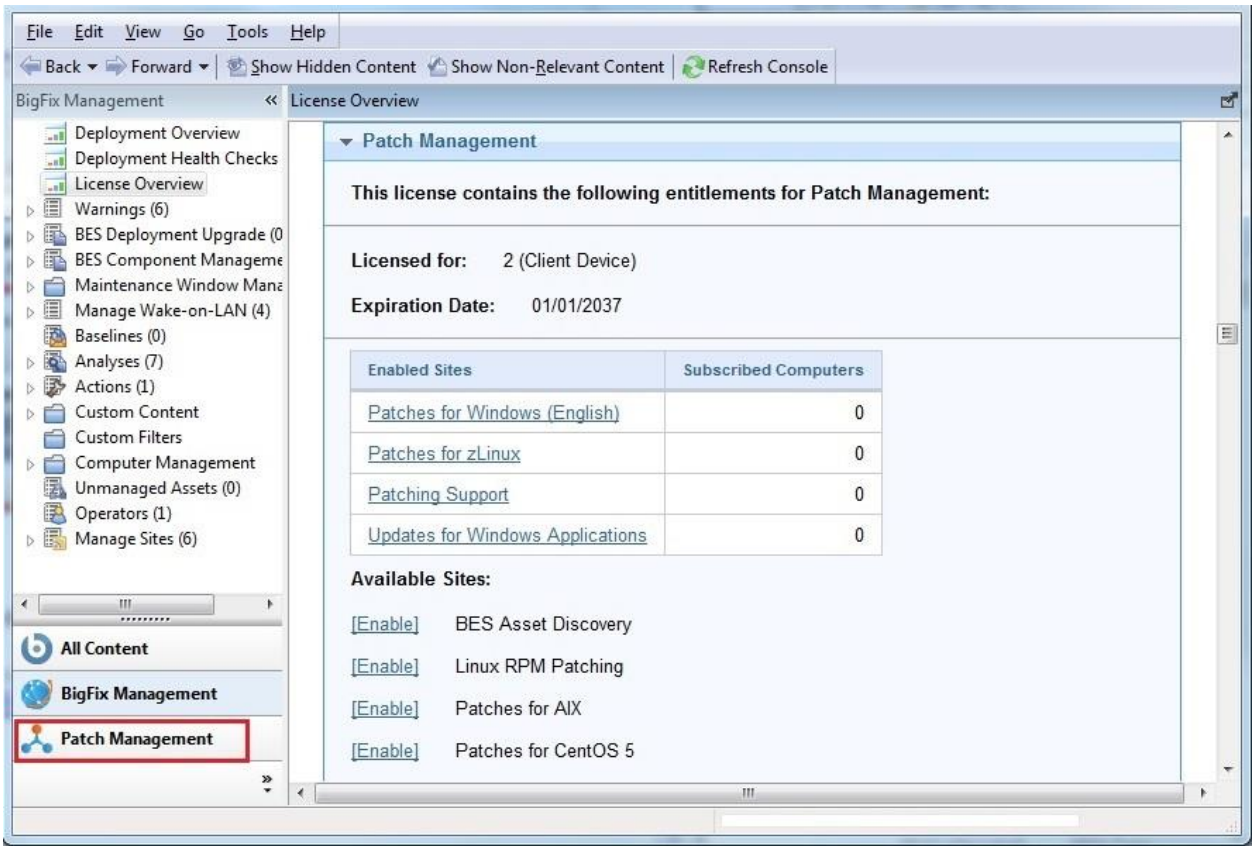

Рис. 1. Консоль управління виправленнями BigFix

Сайт *Patch Management* тепер буде відображатися в *Manage Sites* вузла панелі домена.

Необхідно відкрити *Manage Sites* та обрати *Patches for Windows (English)*. У діалоговому віконці необхідно клікнути *Computer Subscriptions tab* та обрати *All computers*. Оператор може дочекатися автоматичного запуску процесу збору або натиснути кнопку *Gather* щоб розпочати завантаження доступного контенту з вибраних сайтів. Після завершення процесу збору *Patches for Windows (English)* заповнюється новим контентом.

Застосування патча Windows

Оператор має виконати такі дії з консолі, щоб застосувати виправлення Windows: розгорнути піддерево *Patches for Windows (English)* натиснути *Subscribed Computers.* На панелі *List* можна побачити запис, що представляє клієнта, встановленого в серверній системі. Виберіть вкладку Relevant Fixlets and Tasks, щоб відобразити список Fixlets, що мають відношення до вибраного клієнта (рис. 2). Fixlet є важливим для клієнта, якщо йому потрібно встановити контент, на який посилається Fixlet. Необхідність встановлення цього контенту автоматично оцінюється на клієнті за допомогою набору заздалегідь визначених умов, зазначених у Fixlet. Двічі натискаючи Fixlet оператор отримує доступ до опису Fixlet. На панелі *Actions* оператор обирає та ініціює процес розгортання.

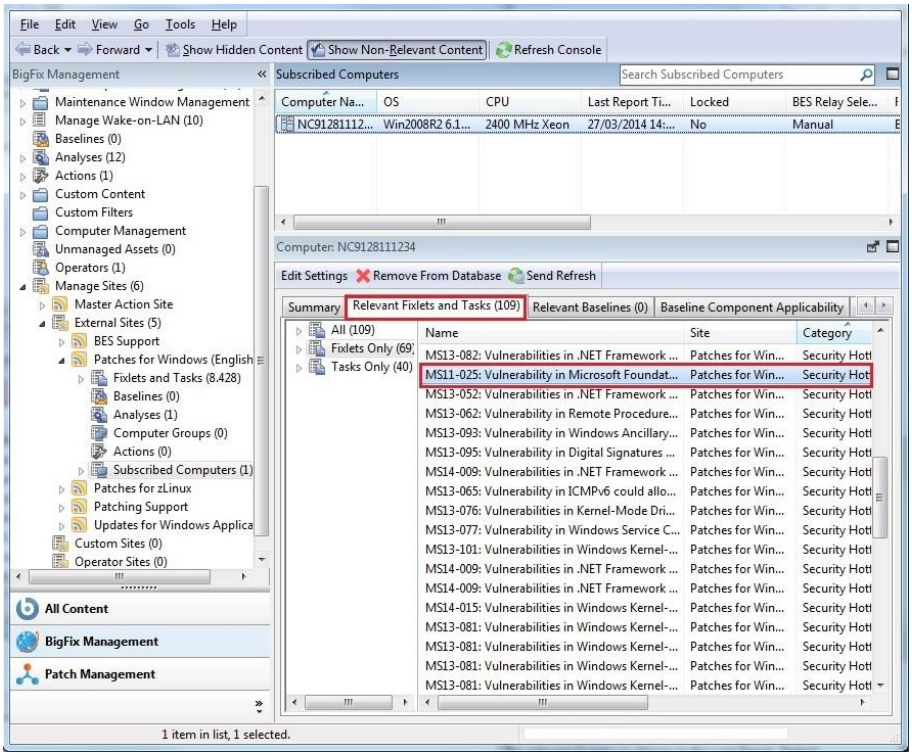

Рис. 2. Вкладка Relevant Fixlets and Tasks

Відкриється панель *Take action*. На цій панелі оператор має брати клієнт, а потім натиснути кнопку *OK*, щоб розпочати розгортання. Оператор буде автоматично перенаправлений на вкладку *Action*. Панель стану показує хід розгортання Fixlet. Статус змінюється з *Not evaluated* на *Evaluating* та *Fixed* (рис. 3), якщо вразливість на клієнті успішно виправлена. Видалення вразливості автоматично обчислюється на *Client* за допомогою набору заздалегідь визначених умов, зазначених на вкладці *Success Criteria* в *Action*.

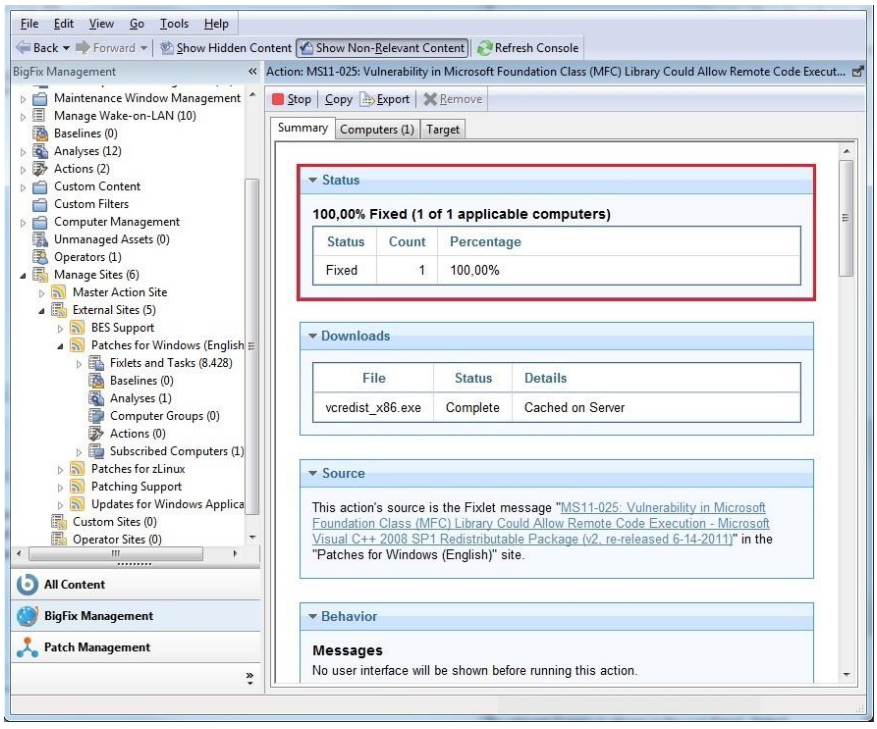

Рис. 3. Вкладка статусу розгортання патча

Після усунення вразливості клієнту не потрібно повторно застосовувати відповідний Fixlet та цей Fixlet помічається як нерелевантний для цього клієнта. Таким чином, в даному підрозділі розглянуто зміст технології управління оновленнями та виправленнями на базі рішення BigFix Patch, якої має дотримуватися оператор безпеки.

Інтеграція IBM QRadar Vulnerability Manager та HCL BigFix

IBM QRadar Vulnerability Manager може інтегруватися з HCL BigFix для надання допомоги фахівцям щодо фільтрації і визначення пріоритетів вразливостей, які можуть бути виправлені.

Розглянемо можливості рішення HCL BigFix з керування вразливостями. Рішення HCL BigFix забезпечує загальний огляд і контроль IT-операцій і безпеки. HCL BigFix застосовує Fixlets до вразливостей з високим пріоритетом, які виявляються і відправляються QRadar Vulnerability Manager в BigFix. Fixlets це пакети, які оператори розгортають на своїх ресурсах або кінцевих точках для усунення певних вразливостей. Оператор можете одночасно розгортати Fixlets на багатьох активах або кінцевих точках з панелі управління «Управління вразливими комп'ютерами» на консолі BigFix. Вкладка «Управління вразливими комп'ютерами» на консолі BigFix застосовується оператором для управління і контролю мережі з сотень тисяч активів або кінцевих точок на різних платформах і пристроях, що знаходяться в будь-якому географічному місці.

BigFix надає панель управління, яка може бути інтегрована з QRadar Vulnerability Manager. Ця панель управління на консолі BigFix використовується для перегляду і усунення вразливостей, виявлених і відправлених QRadar Vulnerability Manager. Щоб переглядати дані про вразливість QRadar Vulnerability Manager в консолі BigFix, необхідно налаштувати QRadar Vulnerability Manager, а потім налаштувати BigFix для обробки даних про вразливість, що відправляються з QRadar Vulnerability Manager.

Розглянемо порядок усунення усунення вразливості. Залежно від того, чи встановлено і інтегровано BigFix, QRadar Vulnerability Manager надає наступну інформацію про вразливості. Якщо BigFix не встановлено, QRadar Vulnerability Manager надає щоденні оновлення про вразливість, для яких це виправлення доступне. QRadar Vulnerability Manager веде список інформації про виправлення вразливостей. Інформація про виправлення зіставляється з каталогом відомих вразливостей.

Використовується пошук в QRadar Vulnerability Manager, щоб визначити вразливості, для яких є доступні виправлення. Якщо встановлений BigFix, QRadar Vulnerability Manager також надає конкретні відомості про процес виправлення вразливостей. Наприклад, може бути заплановано виправлення або актив може бути вже виправлений. Сервер BigFix збирає інформацію про виправлення від кожного з агентів BigFix. QRadar Vulnerability Manager отримує оновлення інформації про виправлення вразливостей з сервера BigFix через заздалегідь задані інтервали часу. Використовується пошук в QRadar Vulnerability Manager, щоб визначити вразливості, які планується виправити або які вже виправлені.

Типове інтегроване розгортання складається з таких компонентів: консоль IBM QRadar; QRadar Vulnerability Manager; сервер BigFix; агент BigFix кожної кінцевої точки для їх сканування в корпоративній мережі.

Перед налаштуванням інтеграції між IBM QRadar і BigFix важливо зрозуміти, як вони взаємодіють один з одним.

На рис. 4 показано загальний огляд деяких взаємодій між QRadar і BigFix від початкового сканування активів до усунення вразливостей в просканованих активах. Далі описується загальний план взаємодії між QRadar і BigFix від початкового сканування вразливостей до усунення цих вразливостей:

Сканер QRadar Vulnerability Manager виконує сканування активів з перевіркою достовірності для виявлення вразливостей. BigFix може обробляти тільки вразливості активів, налаштованих в профілях сканування, що використовують політики сканування Full, Patch або PCI. Якщо агент BigFix встановлений на активі, QRadar Vulnerability Manager

витягує *BES agent ID* з активу, коли виявляє вразливості в активі. BES агент ID це унікальний ідентифікатор, який використовується BigFix для ідентифікації активу і для усунення вразливостей в цьому активі. BigFix називає активи QRadar комп'ютерами.

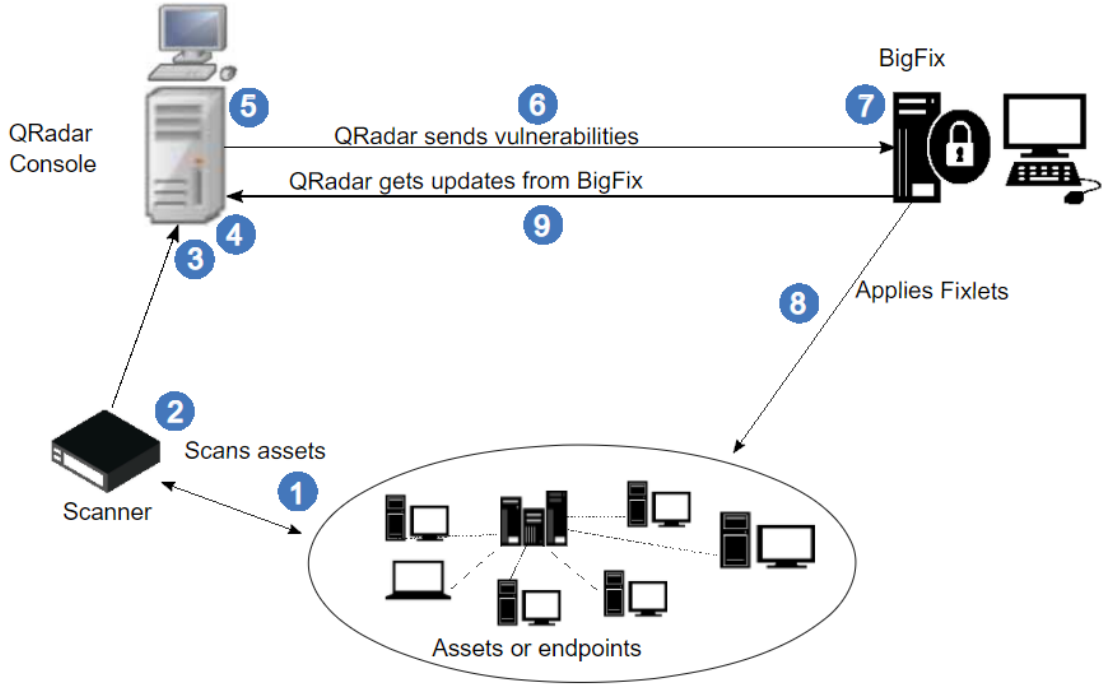

Рис. 4. Взаємодія QRadar Vulnerability Manager та BigFix [14]

Результати сканування оновлюються в моделі активів QRadar, яка включає *BES agent ID* з будь-яких активів, у яких є агент BigFix. Коли статус сканування в профілі сканування відображає статус виконання 100%, модель активу оновлюється, і дані про вразливість за замовчуванням відправляються в BigFix протягом 15 хвилин.

Коли модель активу оновлюється даними сканування, адаптер BigFix, встановлений на консолі QRadar, отримує оновлені дані про вразливість з оцінками ризику з моделі активу. Дані містять BES agent ID. BigFix адаптер обробляє тільки інформацію про вразливість від активів, коли BES agent ID включений. Дані про вразливість, що відправляються в BigFix, фільтруються за параметрами оцінки ризику, які налаштовані в файлі властивостей адаптера (*/opt/qvm/adaptor/config/adaptor.properties*) на консолі QRadar. Оцінка ризику за замовчуванням 0.0, що означає, що всі вразливості відправляються в BigFix.

BigFix адаптер використовує BigFix API REST для відправки інформації про вразливість BigFix і корелює з CVEs вразливості з Fixlets. За замовчуванням дані відправляються в BigFix з інтервалом в 15 хвилин. Інформація про вразливість, що відправляється REST API, доступна для перегляду на панелі управління BigFix Manage Vulnerable Computers. Оператор може розгорнути Fixlets на активах з уразливостями з високим рівнем ризику з панелі управління BigFix Manage Vulnerable Computers. BigFix використовує BES agent ID як унікальне посилання для активу, коли застосовує Fixlets безпосередньо до активу. BigFix застосовує Fixlets до активів, які мають уразливості. SOAP API (веб-звіти) використовується для отримання статусу виправлення вразливості від BigFix. Оператор може використовувати збережені пошукові запити і фільтри на вкладці «Вразливості», щоб переглянути оновлену інформацію про вразливість. Оператор повинен повторно просканувати виправлені активи, щоб оновити модель активу з урахуванням зміненого статусу вразливості корпоративних активів. Управління виправленнями є одним з декількох компонентів стратегії багаторівневого захисту, яке також повинне включати проектування захищеної архітектури, інтегроване управління ризиками, планування безперервності бізнесу і функції безпеки, такі як моніторинг і реагування на інциденти [9].

Рекомендації щодо управління оновленнями та виправленнями програмного забезпечення корпоративної інформаційної системи на підприємстві

Існує взаємозв'язок між управлінням вразливостями, конфігурацією і управлінням змінами, а також інвентаризацією і виявленням активів, які є частинами всього процесу управління виправленнями.

Інвентаризація та виявлення активів. Для управління виправленнями потрібні поточна і повна інвентаризація програмного забезпечення організації, включаючи версії і їх розміщення на мережевих вузлах. Загальні функції інвентаризації та виявлення активів або управління активами перетинаються з керуванням вразливостями і більш широкою програмою управління виправленнями. Можливість інвентаризації та виявлення активів включає ідентифікацію додатків на активах, вбудованого ПЗ на пристроях, версій і приписаних вразливостей. Він також надає можливості віддаленого управління, такі як оновлення, установка, видалення тощо. Віднесення активів до систем і здатність відображати критичність бізнесу є визначальними функціями, які можуть допомогти в прийнятті рішень щодо пріоретизації виправлень і термінів розгортання, зокрема впливу на доступність послуг.

Управління вразливостями. Сканування вразливостей та їх оцінка (VA) є елементами управління вразливостями і фундаментальної залежністю для управління виправленнями. Ця залежність, з точки зору процесу управління виправленнями, перетинається з інвентаризацією і виявленням активів для зіставлення інвентаризацій програмного забезпечення з виявленими вразливостями.

Необхідно застосовувати *автоматичне сканування мережевих систем* за допомогою віртуального пристрою підприємства дає наступні переваги [9]:

повідомлення про пріоритети розгортання виправлень для готового комерційного програмного забезпечення (COTS);

виявлення та кількісна оцінка рівня схильності та визначення результуючого ризику від явних вразливостей;

визначення показників ефективності управління виправленнями з плином часу, що, в свою чергу, дозволяє організації підвищити ефективність і результативність своєї програми управління виправленнями.

Конфігурація та управління змінами. Оновлення програмного забезпечення є зміною конфігурації, яке слід враховувати в процесі управління конфігурацією і змінами.

Ключові показники ефективності. Стратегія управління виправленнями повинна включати заходи для KPI, щоб оцінити її результативність і дієвість. Корпоративна система управління виправленнями повинна надавати можливості звітності, що дозволяють проводити вимірювання з плином часу. Деякі приклади KPI включають [9]:

охоплення: відсоток систем і додатків в організації, інвентаризованих і охоплених автоматичним управлінням виправленнями;

ефективність і дієвість: як часто хости автоматично перевіряються на відповідність;

як часто автоматично оновлюються запаси активів;

мінімальний/середній/максимальний час для виправлення X відсотків хостів;

відсоток систем, виправлених протягом X, Y, Z днів після розгортання;

відсоток операційних хостів в організації, на яких в будь-який момент часу були встановлені всі виправлення;

кількість вузлів з екстремальним, високим, середнім і низьким рівнем впливу та/або незахищених вразливостей на вузлах організації в будь-який момент часу;

середній час, що минув між доступністю виправлення і його продуктивною реалізацією, в залежності від рівня рейтингу;

відсоток хостів, виправлених автоматично або частково (в разі виправлень в пакеті) або вручну;

відсоток виправлень, розгорнутих в рамках пропонованого графіка розгортання.

Регулярна звітність по KPI дозволить організації встановити базовий рівень продуктивності свого процесу управління виправленнями і швидко його вдосконалити. Необхідно ретельно налаштувати і протестувати кожен патч перед його розгортанням. В іншому випадку існує ризик порушити роботу критично важливих систем і знизити продуктивність користувачів [10]. Розглянуте та досліджене рішення HCL BigFix Patch забезпечує вичерпні дані та функціональні можливості, необхідні для точної оцінки загроз, які мають місце, надання пріоритетних зусиль на виправлення на основі ризику для бізнесу та швидкого виправлення. Такі рішення, що реалізують технологію Patch management, необхідно застосовувати в корпоративній інформаційні системі.

Висновки

Проведений аналіз проблеми наявності вразливостей корпоративних інформаційних систем показав необхідність впровадження технології управління оновленнями та виправленнями програмного забезпечення. Було визначено та досліджено варіант технології управління оновленнями та виправленнями на базі рішення BigFix Patch, якої має дотримуватися оператор безпеки. У роботі розглянуто порядок інтеграції рішень IBM QRadar Vulnerability Manager та HCL BigFix, знання якого потрібно фахівцям SOC. Розроблено рекомендації фахівцям із кібербезпеки щодо застосування технології управління виправленнями та оновленнями програмного забезпечення корпоративної інформаційної системи на підприємстві.

Таким чином, технологія управління виправленнями та оновленнями програмного забезпечення є важливою складовою забезпечення кібербезпеки інформаційних систем підприємства. Централізоване управління виправленнями та оновленнями програмного забезпечення спрощує роботу адміністраторів безпеки, підвищує якість даного процесу та скорочує час їх втілення в активи, що безпосередньо впливає на кількість вразливостей, які мають місце в корпоративній інформаційній системі.

Перелік посилань

1. X-Force Threat Intelligence Index 2020. Produced by IBM X-Force Incident Response and Intelligence Services (IRIS) [Електронний ресурс] – Режим доступу: https://www.ibm.com/security/digital-assets/xforce-threat-intelligence-index-map/#/.

2. National Institute of Standards and Technology, «Guide to Enterprise Patch Management Technologies SP 800-40 Rev. 3», 2013. [En ligne]. Available: https://csrc.nist.gov/publications/detail/sp/800-40/rev-3/final.

3. Patch Management. Тестирование ежемесячных обновлений ПО. ICL Services. Цифровые технологии для бизнеса [Електронний ресурс] – Режим доступу: https://habr.com/ru/company/icl_services/blog/251575/.

4. BigFix Patch. Continuous patch compliance,visibility and enforcement [En ligne]. Available: https://www.hcltechsw.com/wps/wcm/connect/b9e1f43e-3aa9-4290-badd-42975410e9cb/HCL+BigFix+-+Datasheet+-+Patch+-+v1.2.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=ROOTWORKSPACE-b9e1f43e-3aa9-4290-badd-42975410e9cb-niwotd1.

5. Скрябін Ф.К. Технологія управління виправленнями та оновленнями програмного забезпечення корпоративної інформаційної системи на базі рішення HCL BigFix Patch /Ф.К. Скрябін // Всеукраїнська наукова конференція «Актуальні проблеми кібербезпеки». Тези доповідей. 22 жовтня 2020 року, м. Київ – с. 49-51.

6. Прикриттям наймасштабнішої кібератаки в історії України став вірус Petya (Diskcoder.C). 05 липня 2017 р. [Електронний ресурс] – Режим доступу: https://cyberpolice.gov.ua/news/prykryttyam-najmasshtabnishoyi-kiberataky-v-istoriyi-ukrayiny-stav-virus-diskcoderc-881/.

7. Anton Cherepanov. Analysis of TeleBots' cunning backdoor. 4 Jul 2017 [Електронний ресурс] – Режим доступу: https://www.welivesecurity.com/2017/07/04/analysis-of-telebots-cunning-backdoor/.

8. HCL Software. Product Documentation. A patch management scenario [En ligne]. Available: https://help.hcltechsw.com/bigfix/10.0/platform/Platform/Getting_Started/c_user_scenario.html.

9. Patch Management Guidance. From: Treasury Board of Canada Secretariat [En ligne]. Available: https://www.canada.ca/en/government/system/digital-government/online-security-privacy/patch-management-guidance.html

10. A constantly evolving solution for an ever-changing threat environment. Protecting your IT estate from software vulnerabilities. eBook [En ligne]. Available: https://www.demandtalk.com/whitepaper/security/protect-your-it-estate-from-software-vulnerabilities.

Надійшла: 16.09.2021 Рецензент: д.т.н., професор Савченко В.А.