Попередження та виявлення кібератак на мережеві пристрої

Колін Дуган (Colin Duggan), BG Networks
Переклад та редагування: Роман Горєлков

У цій статті розглядаються правила та найкращі практики кібербезпеки пристроїв Інтернету речей.

Захист пристроїв Інтернету речей від кібератак — це питання боротьби з потенційними ризиками. Деякі вразливості виникають через відсутність належних вбудованих заходів безпеки, таких як безпечний зашифрований зв'язок, безпечне завантаження та безпечне оновлення програмного забезпечення. Інші є наслідком використання слабких паролів (стандартних або таких, які легко зламати). Вирішення цих проблем вимагає належного впровадження відповідних засобів безпеки.

Складнішою проблемою є усунення вразливих місць у системі безпеки, які виникають, коли при розробці продукту використовуються рішення з відкритим кодом (*open-source*) або комерційні рішення сторонніх розробників. Ці компоненти можуть містити вразливі місця, про які розробник не знає. Пристрої Інтернету речей все більше покладаються на поєднання програмного забезпечення власної розробки, програмного забезпечення з відкритим кодом та комерційного програмного забезпечення від сторонніх постачальників.

Це створює складний ланцюг постачання програмного забезпечення з широким фронтом для атак, яким можуть скористатися зловмисники. Вкрай важливо відстежувати вразливі місця в цих програмах, а найкраща практика полягає у тому, щоб додати моніторинг і звітність в режимі реального часу для забезпечення глибокого захисту ланцюга постачання.

Існують нові правила і стандарти, які встановлюють вимоги до кібербезпеки для пристроїв Інтернету речей. Ось деякі з них, про які повинні знати розробники пристроїв Інтернету речей:

- UNECE Regulations UN R155 & UN R156 [2] for Vehicle Cybersecurity;
- ISO 21434 Road Vehicle Cybersecurity Standard;
- Cybersecurity in Medical Devices: Refuse to Accept Policy from March 29, 2023;
- EU MDR Medical Device Regulation;
- ISA/IEC 62443 and NIST Cyber Security Framework (CSF) guidelines for the security of industrial automation and control systems;
- UK Product Security and Telecommunications Infrastructure Act 2022;
- EU Cybersecurity Resilience Act.

АТАКИ НА ЛАНЦЮГИ ПОСТАЧАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Безпека ланцюгів постачання програмного забезпечення не є чимось новим, але зараз вона стає ще більш важливою, ніж будь-коли. Її важливість підкреслюють кілька нещодавніх атак на ланцюги постачання програмного забезпечення, що мали значні наслідки.

У 2019 році зловмисники проникли в мережі SolarWinds та інтегрували шкідливе програмне забезпечення всередину програмного компонента під назвою Orion. Потім, починаючи з березня 2020 року, це шкідливе програмне забезпечення несвідомо поширювалося як законне оновлення SolarWinds з цифровим підписом. Атака на ланцюг постачання програмного забезпечення залишалася непоміченою до грудня 2020 року, що надало змогу зловмисникам отримати місяці невиявленого доступу до уражених систем.

Атака на SolarWinds є прикладом злому ланцюга постачання, коли зловмисники цілеспрямовано вставляють шкідливий код на верхньому рівні ланцюга постачання. Однак, порушення безпеки ланцюга постачання програмного забезпечення також може бути викликане використанням програмного забезпечення з відкритим кодом, що містить вразливі місця.

Log4Shell — це вразливість у бібліотеці Log4J в Apache, яка дозволяє зловмисникам виконувати довільний код на уражених пристроях та системах. Хоча це вразливе місце існувало в бібліотеці Log4j з 2013 року, публічно про нього стало відомо лише в грудні 2021 року. Того ж місяця були виявлені атаки, що використовували цю вразливість.

Оскільки Log4j широко використовувалася як стандартний метод ведення журналів для Java-додатків, знайти всі випадки його використання в корпорації було дуже складною задачею. Особливо це стосувалося випадків, коли програмний додаток не мав списку програмних компонентів, які в ньому використовувалися.

БЕЗПЕКА ЛАНЦЮГА ПОСТАЧАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

У травні 2021 року, у відповідь на гучні кібератаки, такі як атака SolarWinds, президент США видав указ № 14028, у якому були окреслені вимоги до кібербезпеки. Цей указ, зокрема, містить директиви щодо надання рекомендацій та встановлення стандартів безпеки для ланцюга постачання програмного забезпечення. Згодом Національний інститут стандартів і технологій (*National Institute of Standards and Technology, NIST*) випустив оновлення до свого базового документа з керування ризиками

в ланцюгах постачання в спеціальній публікації NIST SP 800-161r1 під назвою «Практика керування ризиками кібербезпеки в ланцюгах постачання для систем і організацій».

Ключовим елементом настанов NIST є вимога до постачальників програмного забезпечення вести специфікацію компонентів програмного забезпечення (*Software Bill of Materials, SBOM*) [1]. SBOM слугує «харчовою етикеткою» для програмного забезпечення, визначаючи всі його «інгредієнти» та надаючи важливу інформацію (наприклад, номер версії, умови ліцензування) про кожен компонент (рис. 1). SBOM можна використовувати для визначення наявності відомих вразливостей у програмному забезпеченні, оцінки доступності оновлених версій програмного забезпечення та перевірки цілісності завантаженого програмного забезпечення.

Dependency Track [2], безкоштовне рішення з відкритим кодом, є однією з декількох платформ для аналізу SBOM, яка дозволяє розробникам програмного забезпечення безперервно аналізувати своє програмне забезпечення. Ці платформи автоматично порівнюють бази даних вразливостей зі SBOM і генерують звіти про відомі вразливості, наявні у збірці програмного забезпечення. Автоматизація має вирішальне значення для налагодження процесів, які ефективно використовують інформацію SBOM на постійній основі (наприклад, кожного разу, коли з'являється нова збірка).

Рис. 1. Ланцюг постачання програмного забезпечення для продуктів IoT є складним, що створює труднощі з відстеженням усіх компонентів

АВТОМАТИЗАЦІЯ БЕЗПЕКИ ЛАНЦЮГА ПОСТАЧАННЯ

Для розробників програмного забезпечення для IoT ефективне створення SBOM, який визначає всі залежності програмного забезпечення в межах збірки, є складним завданням. Підтримка автоматичної побудови SBOM з використанням стандартних форматів є неузгодженою в різних системах збірки. SPDX і CycloneDX є двома провідними форматами SBOM, але багато інструментів підтримують лише один з них. Це призводить до несумісності між системами збірки та інструментами для аналізу SBOM.

SPDX спочатку був створений для керування ліцензіями на відкрите програмне забезпечення, в той час як CycloneDX був розроблений для створення SBOM з метою керування вразливостями. Однак, їх функціональність зблизилася, і тепер обидва інструменти дозволяють створювати SBOM. Є дві причини, чому розробник IoT може обрати SPDX замість CycloneDX:

- SPDX є більш поширеним і наразі підтримується більшою кількістю інструментів;
- SPDX має сильний компонент ліцензування, що важливо при використанні програмного забезпечення з відкритим кодом у комерційних продуктах.

Інтеграція систем збирання з інструментами аналізу SBOM є дуже важливою. Ці інструменти не тільки виявляють відомі вразливості під час збірки, але й постійно відслідковують бази даних на предмет нових виявлених вразливостей. Якщо у використовуваному вами компоненті виявлено нову вразливість, буде згенеровано сповіщення, що дозволить вам завчасно вирішити проблему.

Одним з таких інструментів для розробників IoT є Vulnerability Scanning [3] компанії BG Networks для вбудованого Linux. Цей інструмент інтегрується з системою керування збірками Yocto для автоматичного створення SBOM для кожної нової збірки. Потім він використовує Dependency Track для пошуку відомих вразливостей, гарантуючи, що програмні проєти відповідають рекомендаціям NIST щодо безпеки ланцюга поставок.

ЗАХИЩЕНІСТЬ ПРИСТРОЇВ ТА ЗМЕНШЕННЯ ВРАЗЛИВИХ МІСЦЬ У ЛАНЦЮГАХ ПОСТАЧАННЯ

Аналіз ланцюга постачання може виявити відомі вразливі місця в програмному забезпеченні пристроїв Інтернету речей і навіть надати інформацію про наявність нових версій цих програм, що містять виправлення для усунення цих вразливостей.

Досить часто оновлені версії програмного забезпечення містять виправлення відомих вразливих місць. Тому у таких випадках оновлення до більш нової версії усуває вразливість. В інших випадках розробникам може знадобитися вирішити проблему за допомогою самостійного корегування коду чи використання альтернативного програмного рішення.

Інколи оновлення до новішої версії програмного забезпечення не усуває всі відомі вразливості. Гірше того, невідомі вразливості майже напевно залишаться у великій та складній системі. Наприклад, вразливість Log4j залишалася невиявленою протягом багатьох років до того, як її було виявлено. Захист пристроїв від таких вразливостей потребує додаткових заходів безпеки.

Оскільки кожен пристрій Інтернету речей є унікальним, необхідно провести оцінку загроз/аналіз ризиків (*Threat Assessment/Risk Analysis, TARA*), щоб керувати розробкою засобів захисту для кожного пристрою. Поширені вразливі місця в безпеці пристроїв Інтернету речей варіюються від відсутності фундаментальних засобів контролю безпеки, передових практик до вразливих місць у ланцюгу поставок програмного забезпечення (табл. 1). Хоча TARA надає конкретні рекомендації для кожного пристрою, кілька загальних принципів застосовуються до всіх пристроїв IoT. Кожен IoT-пристрій повинен мати такі мати такі інструменти та можливості для забезпечення безпеки:

- апаратний RoT (*Root of Trust*);
- безпечне завантаження;

Таблиця 1. Поширені вразливі місця в безпеці пристроїв Інтернету речей

Вразливість безпеки	Опис
Відсутність засобів контролю безпеки	Інтерфейси без засобів контролю безпеки (наприклад, неавторизовані веб-інтерфейси, неавторизовані оновлення прошивки)
Слабка автентифікація	Паролі за замовчуванням або слабкі паролі. Застаріле, вразливе шифрування (наприклад, TripleDES, хешування MD-5, SHA-1, RSA-512)
Ланцюг постачання	Будь-яка вразливість, що виникла внаслідок використання програмного забезпечення з відкритим кодом або стороннього програмного забезпечення, яке містить вразливості
Помилки в програмному абезпеченні	Помилки в програмному забезпеченні, що призводять до переповнення буфера або інших помилок, які можуть бути використані хакерами

- безпечне оновлення програмного забезпечення/прошивки;
- криптографічно надійна ідентифікація пристрою;
- безпечні протоколи зв'язку;
- шифрування критично важливих даних у стані спокою.

Впровадження всіх цих функцій безпеки може бути складним і тривалим процесом. Час виходу на ринок часто має вирішальне значення, що призводить до необхідності усунення непотрібних функцій. На жаль, це часто призводить до того, що продукти випускаються без критично важливих функцій безпеки. Були розроблені нові рішення, такі як Security Automation Tool від BG Networks [4], які автоматизують реалізацію багатьох з цих функцій безпеки. Використовуючи такі інструменти, час розробки ключових функцій безпеки можна скоротити до декількох тижнів.

ВИЯВЛЕННЯ АТАК НА ПРИСТРОЇ ІНТЕРНЕТУ РЕЧЕЙ В РЕЖИМІ РЕАЛЬНОГО ЧАСУ

Використання аналізу ланцюгів поставок та захист пристроїв Інтернету речей критично важливими функціями безпеки є значним кроком у створенні безпечних IoT-пристроїв. Ці кроки суттєво зменшують кількість вразливих місць, якими можуть скористатися потенційні хакери. Однак, незалежно від того, наскільки ретельно працює команда розробників, жоден пристрій не буде ідеально захищеним.

Пристрої Інтернету речей мають вразливі місця і неминуче будуть атаковані, тому для їх виробників вкрай важливо мати інформацію про атаки на їхні пристрої. Виявлення атак в режимі реального часу та реагування на них є основою будь-якого рішення для забезпечення безпеки підприємства. Аналогічно, пристрої Інтернету речей повинні мати змогу виявляти атаки та сповіщати при здійсненні на них атаки.

Програмне рішення для виявлення аномалій на базі хоста, таке як AnCyR [5] від BG Networks, поєднує в собі статистичні, ймовірнісні та алгоритми машинного навчання для точного виявлення атак з низьким рівнем помилкових спрацьовувань. Використаний у якості програмного агента AnCyR будує модель роботи програмного забезпечення пристрою Інтернету речей. Після завершення етапу навчання він відстежує виконання програмного забезпечення на пристрої та виявляє будь-які відхилення від очікуваної моделі.

Кібератаки змінюють поведінку програмного забезпечення на пристрої, тому будь-яка зміна потенційно є кібератакою. При виявленні атаки рішення надсилає сповіщення до системи керування інформацією та подіями безпеки (*Security Information and Event Management, SIEM*) або іншого рішення для моніторингу мережі.

Розроблене для використання в малогабаритних пристроях Інтернету речей, рішення працює з мінімальними затратами. Воно може функціонувати з лише десятками кілобайт пам'яті та використовує менш ніж 10% обчислювальної потужності на обробку даних.

У корпоративному світі такі рішення відомі як виявлення та реагування на кінцеві точки (*Endpoint Detection and Response, EDR*). Еквівалентним терміном для IoT є рішення для виявлення/запобігання вторгнення (*Intrusion Detection/Prevention Solutions, IDPS*). Коли пристрій стає об'єктом кібератаки або компрометації, в результаті чого зловмисник отримує контроль над пристроєм або експортує дані, його поведінка змінюється. Він може запускати шкідливе програмне забезпечення у якості частини DDoS-мережі чи мережі ботів для крипто-майнінгу, експортувати приватні дані або брати участь в інших зловмисних діях.

Виявляючи та повідомляючи про таку аномальну поведінку, оператори мереж можуть вжити заходів для зменшення та запобігання поширенню кібератак на об'єкти критичної інфраструктури. Це важливий додатковий рівень безпеки. Він не замінює такі функції, як безпечне завантаження та безпечний зв'язок, і не усуває потреби в захисті ланцюга постачання. Скоріше, він забезпечує захист в режимі реального часу від будь-яких вразливих місць, що залишилися, навіть тих, про які розробники ще не знають.

ПІДСУМОК

Сучасне законодавство та галузеві стандарти вимагають від виробників активної участі у забезпеченні безпеки своїх пристроїв. Законодавчі вимоги в автомобільній промисловості зобов'язують дотримуватися рекомендацій з кібербезпеки всіх, хто хоче продавати автомобілі в Європі. У США FDA вимагає від компаній-виробників медичного обладнання впроваджувати заходи кібербезпеки. Споживчий, енергетичний та промисловий ринки мають свої власні стандарти, яких необхідно дотримуватися.

Ці нові правила призвели до значного прогресу у сфері кібербезпеки для пристроїв Інтернету речей. Багато нових пристроїв тепер використовують безпечне завантаження, безпечне оновлення програмного забезпечення, надійну ідентифікацію та захищені протоколи зв'язку, що допомагає захистити ці пристрої від кібератак. Керування безпекою ланцюга постачання та виявлення атак в режимі реального часу також необхідні для забезпечення безпеки цих пристроїв.

Для того, щоб переконатися, що пристрій захищений і відповідає вимогам кібербезпеки, необхідно провести TARA для пристрою, забезпечити безпеку ланцюга поставок та впровадити ключові функції кібербезпеки. Впровадження функцій кібербезпеки може зайняти багато часу, але автоматизовані інструменти допомагають значно полегшити цей процес для розробників.

Література:

1. https://www.linuxfoundation.org/webinars/generating-software-bill-of-materials
2. https://dependencytrack.org/
3. https://bgnetworks.com/vulnerability-scanning/
4. https://bgnetworks.com/bgn-sat/
5. https://bgnetworks.com/ancyr/

CN