ОЦІНКА ВРАЗЛИВОСТЕЙ СИСТЕМ, ПОБУДОВАНИХ ПО ТЕХНОЛОГІЇ ІНТЕРНЕТ РЕЧЕЙ ЗА МЕТОДИКОЮ CVSS

Ліхота О.І.
Науковий керівник – Немченко В.П.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки,14, Кафедра автоматизації проектування обчислювальної техніки, тел. (057) 702-13-06,
e-mail: oryna.likhota@nure.ua

The purpose of my work was to analyze the vulnerabilities that can occur in any device using Internet technology. An analysis of the threats that were detected in the device, such as the ThingsPro Suite the IIoT gateway and device manager from the company Moxa, was carried out. After analysis, the risk of information security was calculated using the CVSS methodology.

Загальна система оцінювання вразливостей (CVSS) – це вільний і відкритий галузевий стандарт для оцінки рівня вразливостей системної безпеки комп'ютера. CVSS намагається визначити оцінку ступеня вразливостей, що дозволяє респондентам визначити пріоритети захисту відповідно до загроз. Оцінки розраховуються на основі формули, яка залежить від кількох показників, що наближають простоту використання та вплив експлуатації.

Кібератаки з використанням вразливостей, що були проаналізовані:

- отримання автентифікаційних даних користувача;
- підвищення привілеїв;
- виконання довільного коду;
- підвищення привілеїв всередині системи;

Особливість вразливості «Отримання автентифікаційних даних користувача» полягає у тому, що У зловмисника є можливість спробувати отримати підтвердження того, що користувач існує в системі. Вона полягає в тому, що з відповідей від сервера на отримані ним дані автентифікації можна визначити, існує користувач в системі чи ні.

А вектор атаки: [AV:N/ AC:L/ AU:S/ C:C/ I:N/ A:N]. А загальна оцінка загрози: 6.8

Щодо вразливості «Підвищення привілеїв», то тут проблема полягає у тому, що Автентифікований користувач ThingsPro Suite в веб-панелі може змінювати дані свого облікового запису. Серед цих даних - логін, пароль, адресу електронної пошти та назву компанії. Для зміни цих даних веб-сервісу відправляється HTTP-запит. Після зміни значення role з user на root і повторної відправки повідомлення, у відповіді сервера було зазначено, що роль поточного користувача змінена з user на root.

Вектор атаки: [AV:N/ AC:L/ AU:S/ C:C/ I:C/ A:C]. Загальна оцінка: 9.0.

Атака «Виконання довільного коду». Для користувача з високим рівнем привілеїв в ThingsPro Suite доступна функціональність, яка змінює

системні настройки або поведінку ThingsPro Suite в цілому. Для обробки такого рівня запитів веб-додаток змушений звертатися до можливостей командного рядка операційної системи Linux.

Вектор атаки: [AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N]. Загальна оцінка: 9.0.

І остання атака «Підвищення привілеїв всередині системи». Як правило, для розвитку атаки на веб-сервер після отримання доступу до командної оболонки Linux потрібне підвищення привілеїв, тому що зазвичай веб-сервери запускаються з-під окремо створеного в системі користувача з обмеженими правами. Так працює, наприклад, apache або nginx. Однак, веб-сервер ThingsPro Suite вже запущений з-під користувача root в системі, тому, отримавши можливості виконання довільних команд, зловмисникові підвищувати привілеї не треба.

Вектор атаки: [AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N]. Загальна оцінка: 9.0.

У висновках можна сказати, що технологія «Інтернет речей» ще дуже молода, тож більшість загроз, що існують через те, що розробники занадто швидко випускають нові продукти, та не тестують їх належним образом. У всіх на меті лише якомога швидше стати лідерами у цій сфері. То ж, де, як не в цій сфері потрібен добрий аналіз загроз та повне розуміння ризиків інформаційної безпеки. Як було виявлено в атестаційній роботі, облікові дані для перевірки автентичності в хмарі, які використовуються в процесі настройки та експлуатації розгортання IoT, мабуть, являють собою найсерйознішу уразливість, яку зловмисники можуть легко використовувати, щоб отримати доступ до системи IoT і скомпрометувати її. Для захисту облікових даних рекомендується регулярно міняти пароль і намагатися не використовувати ці облікові дані на загальнодоступних комп’ютерах.

З аналізу можна зробити такі висновки. Компаніям треба більш ретельно підходити до тестуванню свого програмного забезпечення та приладів, та розраховувати усі ризики, що можуть бути. Так як, усі загрози, що були виявлені – це лише результати занадто швидкої розробки продукту.

Щоб забезпечити належний рівень безпеки для інфраструктури IoT, необхідна стратегія всебічного захисту. В рамках неї забезпечується захист даних в хмарі, захист цілісності даних при передачі в Інтернет, а також безпечне виробництво пристроїв. І все це дуже залежить від доброго аналізу усіх вразливостей та ризиків.

Список використаних джерел:

1. Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology [Електронний ресурс]. – 2002. – Режим доступу до ресурсу: http://csrc.nist.gov/publications/nistpubs/.