УДК 004.057.4:355.451]:004.75

ОГЛЯД ВРАЗЛИВОСТЕЙ МЕРЕЖНОГО ОБЛАДНАННЯ В ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Назаров Байрамалі Аріф
Науковий керівник – д.т.н., проф. Євдокименко М.О.
Харківський національний університет радіоелектроніки,
каф. ІКІ ім. В.В. Поповського
Харків, Україна
тел. +38(068) 420-39-29.

There are currently no secure information systems and networks. This is due to the fact that each network equipment and software has a certain list of vulnerabilities. According to the analysis, it was found that the main causes of vulnerabilities are outdated software and non-compliance with the principles of secure software development. Vulnerability management scenarios (plans) must be developed to effectively eliminate network equipment vulnerabilities. These scenarios will include regular testing of patch management coverage of the IT infrastructure, the use of a proactive approach in the elimination of vulnerabilities, and the schedule of updating operating systems and software. With a developed vulnerability management plan and its periodic updates, each company will have a clear strategy for eliminating vulnerabilities and improving security as a whole.

На сьогоднішній день не існує ідеально захищених та безпечних інформаційних систем, які при цьому не знаходяться в ізольованому просторі, а виконують свою бізнес-функцію. Тому навіть у самій надійній та перевіреній системі можуть виявитися вразливості, виявлені як в комунікаційному мережному обладнанні так і в додатках на кінцевих пристроях. Таким чином, при аналізі ризиків інформаційної безпеки треба враховувати вразливості мережного обладнання для мінімізації ризиків як на етапі проектування так і під час функціонування інфокомунікаційної мережі.

Джерелом багатьох вразливостей є застаріле програмне забезпечення (ПЗ), небезпечні протоколі та недотримання принципів безпечної розробки додатків та ПЗ. Для аналізу та врахування найбільшої кількості вразливостей згідно з міжнародним стандартом NIST 800-53 [2], було створено систему загальних вразливостей та ризиків (Common Vulnerabilities and Exposures, CVE), що надає еталонний метод для загальновідомих вразливостей інформаційної безпеки та впливу.

Для охоплення всіх основних характеристик та числової оцінки вразливостей використовується загальна система оцінки вразливості (Common Vulnerability Scoring System, CVSS). Всі ці системи допомагають організаціям належним чином оцінити та визначити пріоритети своїх процесів управління вразливостями.

Згідно аналітичних даних [1] вразливості розподіляються за наступними категоріями щодо їх використання зловмисниками та реалізацією атаки (Рис. 1).

Рисунок 1 – Типи атак, реалізованих за допомогою вразливостей мережного обладнання

Згідно проведеного аналізу, найпопулярнішими та критичними вразливостями в 2022 році є наступні [1,3]:

- Log4j (CVE-2021-44228),
- ProxyNotShell (CVE-2022-41040),
- Spring4Shell (CVE-2022-22965),
- Atlassian Confluence (CVE-2022-26134, CVE-2022-26138),
- Zimbra RCE (CVE-2022-27925, CVE-2022-41352),
- Follina web framework Ruby on Rails (CVE-2022-30190),
- F5 BIG-IP (CVE-2022-1388).

У 2023 році експерти прогнозують, що вразливості Log4Shell, Spring4Shell та подібні до них ще довго залишатимуться загрозою, оскільки системи, що використовують дане вразливе ПЗ, широко поширені.

Висновки: Для ефективного усунення вразливостей мережного обладнання потрібно розробляти сценарії (плани) з управління вразливостями. Дані сценарії включатимуть регулярну перевірку покриття патч-менеджментом ІТ-інфраструктури, застосування проактивного підходу в усуненні вразливостей та графіку оновлення операційних систем та програмного забезпечення. Завдяки розробленому плану з управління вразливостями та його періодичного оновлення кожна компанія матиме чітку стратегію із усунення вразливостей та підвищення безпеки в цілому.

Список використаних джерел:

1. The annual report’22 of the European Union Agency for Cybersecurity, ENISA. The 10th edition, 2023. – 96 p.

2. The NIST Risk Management Framework, NIST Special Publications 800-53, 2022. – 47 p. https://nvd.nist.gov/vuln

3. National Vulnerability Database (NVD). CVSS’22. https://www.nist.gov/