УДК 004.7

Ліщинський В.В., здобувач,
Романець О.А., здобувач,
Марчук Я.В., здобувач,
Рудюк Б.М., асистент
Державний університет «Житомирська політехніка»

БЕЗПЕКА DHCPv6: МЕТОДИ ЗАХИСТУ ВІД АТАК ТА НЕПРАВОМІРНОГО РОЗПОДІЛУ АДРЕС

У сучасних мережевих інфраструктурах із широким впровадженням протоколу IPv6 автоматизовані механізми конфігурації мережевих параметрів набувають особливої важливості. Протокол DHCPv6 відіграє ключову роль, оскільки забезпечує масштабований та гнучкий розподіл IPv6-адрес, налаштувань DNS, інформації про шлюзи та інших параметрів, необхідних для функціонування мережевих вузлів. Проте робота DHCPv6 у відкритому мережевому середовищі створює значні виклики безпеці, адже неконтрольований процес призначення адрес може стати інструментом для різних кібератак, здатних порушити цілісність і доступність корпоративної мережі.

Базовою проблемою DHCPv6 є відсутність механізмів автентифікації між клієнтом і сервером, що відкриває можливість для запуску несанкціонованих серверів, здатних нав’язувати хибні параметри конфігурації. Такі сервери, маскуючись під легітимні, можуть спричинити спрямування трафіку через шкідливі шлюзи, перенаправлення DNS-запитів до сторонніх серверів або повне блокування мережевої доступності.

Ще однією загрозою є перехоплення та модифікація DHCPv6-повідомлень під час передавання. Оскільки традиційна реалізація протоколу не містить механізмів криптографічного захисту, зловмисник може втрутитися в мережевий трафік, змінити конфігураційні параметри або повторно відправити застарілі повідомлення. У мережах, де одночасно застосовуються SLAAC та DHCPv6, з’являються додаткові можливості для маніпуляцій, оскільки зміна RA-повідомлень безпосередньо впливає на те, яким чином клієнт обирає спосіб конфігурації адреси.

Для протидії цим загрозам у корпоративних мережах застосовується комплекс механізмів, які дозволяють контролювати джерела DHCPv6-повідомлень, обмежувати діяльність підозрілих вузлів і запобігати несанкціонованому впливу на конфігураційні процеси. Одним із найбільш дієвих рішень є використання технологій DHCPv6 Shield, що реалізуються на мережевому обладнанні. Вони дозволяють фільтрувати

DHCPv6-трафік залежно від того, з якого порту він надходить, блокуючи відповіді від можливих фальшивих серверів і запобігаючи їхньому впливу на клієнтів. У поєднанні з механізмами RA Guard, які перехоплюють підозрілі оголошення маршрутизаторів, створюється надійний бар'єр для атак, що використовують взаємодію SLAAC і DHCPv6.

Поступово в інфраструктурних рішеннях з'являються можливості використання автентифікації DHCPv6-повідомлень. Цей підхід базується на криптографічних методах перевірки достовірності джерела та цілісності даних, що значно ускладнює підміну серверів або модифікацію трафіку. Додатково важливим засобом є контроль доступу на рівні комутаторів, що передбачає обмеження кількості пристроїв, які можуть ініціювати DHCPv6-запити з одного фізичного порту. Це унеможливлює атаки на виснаження адресного пулу та знижує ризик масових підроблених запитів.

Значну роль у комплексній безпеці відіграють системи моніторингу мережевого трафіку. Інструменти IDS/IPS, журнали DHCPv6-серверів, аналіз аномалій та збір телеметрії дозволяють швидко виявляти підозрілу активність, визначати джерела атак та реагувати на них у реальному часі. IT-адміністратори отримують можливість оперативно блокувати несанкціоновані порти, ізолювати підозрілі пристрої або змінювати конфігураційні політики з метою локалізації загрози.

Таким чином, безпека DHCPv6 є ключовим елементом побудови надійної IPv6-інфраструктури. Наявність кібератак, спрямованих на процеси призначення адрес, вимагає впровадження узгоджених захисних механізмів, які охоплюють фільтрацію трафіку, автентифікацію, моніторинг та розмежування доступу. Застосування таких методів дозволяє організаціям захищати критичні сегменти мережі від підміни конфігураційних сервісів, збоїв у роботі та перенаправлення трафіку. У результаті створюється стійке до атак середовище, у якому процес автоматизованої конфігурації мережевих параметрів залишається керованим, надійним і відповідним сучасним вимогам кібербезпеки.

Список використаних джерел:

1. John RFC 8415: Dynamic Host Configuration Protocol for IPv6 (DHCPv6). *IETF Datatracker*. URL: https://datatracker.ietf.org/doc/html/rfc8415

2. RFC 4861: Neighbor Discovery for IP version 6 (IPv6). *IETF Datatracker*. URL: https://datatracker.ietf.org/doc/html/rfc4861