МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ЛЬВІВСЬКА ПОЛІТЕХНІКА
ЕОМ

Реферат
з дисципліни: «Основи етичного хакінгу**»**
на тему: «Вразливість D-Link NAS»

ст. гр. КІ-403
Порубайміх О.Є.

Львів – 2024

ВРАЗЛИВІСТЬ D-LINK NAS

6 листопада 2024 року на офіційному сайті National Vulnerability Database було опубліковано запис про нову критичну вразливість — CVE-2024-10914, що стосується певних моделей NAS (мережевих сховищ даних) від компанії D-Link. Загалом у світі налічується понад 61 тисячу вразливих одиниць, підключених до Інтернету, що робить проблему ще більш масштабною.

Вразливість виникає внаслідок некоректної обробки параметру *name* в команді *cgi_user_add*, яка використовується в скрипті *account_mgr.cgi* для додавання нових користувачів. Відсутність належної фільтрації введених даних дозволяє зловмиснику впровадити шкідливі команди в систему, що може призвести до виконання довільного коду на сервері. Для експлуатації цієї вразливості досить надіслати простий HTTP GET запит у такому вигляді:

```
curl "http://[Target-IP]/cgi-bin/account_mgr.cgi?cmd=cgi_user_add&name=%27;<INJECTED_SHELL_COMMAND>%27"
```

Де параметр *<INJECTED_SHELL_COMMAND>* замінюється на бажану шкідливу команду, яку зловмисник хоче виконати на сервері. Такі атаки можуть призвести до серйозних наслідків, включаючи компрометацію конфіденційної інформації, порушення цілісності даних або повний контроль над вразливою системою. За допомогою цієї вразливості, зловмисники можуть отримати доступ до системних файлів, змінювати налаштування безпеки або навіть запускати зловмисне програмне забезпечення, що може спричинити тривалий збій у роботі пристроїв.

Ця вразливість вражає кілька моделей мережевих сховищ D-Link, зокрема DNS-320, DNS-320LW, DNS-325 і DNS-340L. Незважаючи на те, що проблема була класифікована як критична, компанія D-Link повідомила, що для цих моделей вразливість не буде виправлена, оскільки термін їх підтримки (EOS) вже завершено. Це означає, що виробник більше не надає оновлення або виправлення для зазначених пристроїв, що ставить користувачів у складну ситуацію, оскільки зростає ризик атак.

У зв'язку з відсутністю патчів для вразливих моделей, користувачі та безпекові експерти вказують на серйозні репутаційні наслідки для D-Link. Компанія вже не вперше стикається з критику щодо безпеки своїх продуктів, і в цій ситуації відмова від виправлення вразливості може призвести до втрати довіри серед користувачів та потенційних клієнтів. Технічні аналітики та спеціалісти з безпеки зауважують, що це може вплинути на продажі нових пристроїв компанії, оскільки споживачі все більше звертають увагу на рівень безпеки продукції перед покупкою.

Реакція користувачів на цю вразливість є неоднозначною. Деякі з них розчаровані тим, що компанія не планує випускати оновлення для вразливих пристроїв, хоча багато хто звернув увагу на запропоновані альтернативи для зниження ризиків, такі як використання сторонніх прошивок або обмеження доступу через брендмауер і NAT. Проте більшість з користувачів вважають, що компанія повинна була б прийняти більш відповідальну позицію і надати рішення для тих, хто використовує ці пристрої.

Не менш важливими є й економічні наслідки для компанії D-Link. Без належної реакції на безпекові інциденти, таких як CVE-2024-10914, виробник ризикує втратити частину ринку. Це може призвести до того, що користувачі NAS пристроїв вибиратимуть конкурентів, чиї продукти мають кращу підтримку безпеки та регулярно оновлюються.

Однак, компанія надала кілька рекомендацій щодо мінімізації ризиків:

1. **Обмеження доступу до Інтернету** для NAS-пристроїв, зокрема шляхом налаштування мережевого транслятора адрес (NAT), що дозволяє обмежити доступ ззовні.
2. **Використання налаштувань брендмауера** для обмеження доступу до девайсів тільки для довірених пристроїв і застосування правил, які можуть зменшити шанси на успішну атаку.
3. **Регулярне оновлення паролів** для доступу до пристроїв і сервісів, щоб ускладнити несанкціонований доступ до системи.

4. **Використання альтернативних прошивок** від сторонніх виробників, що можуть забезпечити додаткові рівні безпеки і підтримку актуальних патчів.

Незважаючи на те, що D-Link не планує випускати оновлення для цих моделей, користувачі повинні активно впроваджувати вищезазначені заходи для забезпечення безпеки своїх пристроїв. Користувачам, які ще не зробили це, рекомендується розглянути можливість заміни вразливих моделей на більш нові пристрої, що підтримують актуальні оновлення безпеки.