

[Home](#) » [Технології](#) » [Хакери отримали доступ до ПК через популярну колонку: чому Creative не випускає виправлення](#)

## Хакери отримали доступ до ПК через популярну колонку: чому Creative не випускає виправлення

**ДМИТРУК АНДРІЙ** — 07 Червня 2026, 09:35 2 Mins Read — [ТЕХНОЛОГІЇ](#)



Creative / Фото з відкритих джерел

Важливі новини щодня — додайте «Експерт» в улюблені джерела Google

У популярній акустиці Creative Sound Blaster Katana V2X виявили серйозні проблеми безпеки, які можуть дозволити зловмисникам атакувати комп'ютери через Bluetooth. Дослідник показав робочий сценарій злому, що діє на відстані до 15 метрів.

Про це повідомляє [v2x](#).

Фахівець із кібербезпеки Расмус Моорац оприлюднив метод експлуатації двох критичних недоліків у системі захисту Sound Blaster Katana V2X. За його словами, Bluetooth Low Energy-інтерфейс саундбара відкриває доступ до протоколу керування будь-якому пристрою поблизу без перевірки автентифікації.

Через це колонка приймає команди радіоканалом навіть у тих випадках, коли вони мали б надходити виключно через захищене USB-з'єднання. Для доступу не потрібні ані паролі, ані попереднє спарювання пристроїв.

Другою проблемою стала відсутність криптографічного підпису офіційних прошивок. Захист оновлень базується лише на контрольній сумі SHA-256, яку можна підмінити.

За сценарієм дослідника, зловмисник у зоні дії Bluetooth може непомітно замінити оригінальне програмне забезпечення колонки на модифіковане. Після цього пристрій додає до конфігурації профіль клавіатури через HID-дескриптор.

Оскільки комп'ютер сприймає саундбар як довірений USB-пристрій, після перезавантаження колонка може автоматично вводити команди та комбінації клавіш. Це відкриває можливість для встановлення шкідливого програмного забезпечення або викрадення даних.

Ситуацію ускладнює те, що Bluetooth-модуль Sound Blaster Katana V2X залишається активним навіть у режимі сну. Пристрій продовжує шукати підключення, залишаючи потенційну можливість для атаки.

Моорац намагався повідомити про проблему виробника, а після відсутності реакції звернувся до сингапурської служби реагування на кіберінциденти SingCERT. Згодом Creative відповіла, що не вважає таку особливість архітектури вразливою та не планує випустити офіційне оновлення безпеки.

У результаті остання офіційна версія програмного забезпечення залишається вразливою до описаного способу атаки.

Як тимчасове рішення дослідник випустив власний інструмент v2x-patcher. Утиліта блокує виконання критичних команд через Bluetooth на рівні мікропрограми.

Водночас автор попереджає, що встановлення такого патча може порушити роботу фірмового мобільного застосунку Creative для смартфонів. Якщо користувачам важлива сумісність із програмою, єдиним способом мінімізувати ризик залишається повне відключення саундбара від електромережі, коли комп'ютер не використовується.

Читайте ЕКСПЕРТ у Google News

ПІДПИСАТИСЯ

Помітили помилку у матеріалі? Повідомте редакцію: [corrections@expert.in.ua](mailto:corrections@expert.in.ua)

[Bluetooth](#) [Creative](#) [кібербезпека](#)

### ОСТАННІ НОВИНИ

#### СЬОГОДНІ

10:14 Пенсійний фонд попередив українців: кому доведеться платити за вихід на пенсію

10:07 Експерти пояснили, як коти реагують на обійми та поцілулки: що відчувають улюбленці

10:06 Назвали регіони з найнижчими результатами з української мови: що показало тестування школярів

09:57 У Раді розкрили новий план мобілізації: скільки хочуть платити іноземним бійцям

09:54 Названо спосіб приготувати яйце пашот за хвилину: плита для цього більше не потрібна

09:49 Названо італійський острів, де поєдналися море, шопінг і краєвиди: чим він приваблює туристів

09:44 Продають кошенят через інтернет: податкова взялася за українців із популярним підробітком

09:35 Хакери отримали доступ до ПК через популярну колонку: чому Creative не випускає виправлення

09:29 Вчені попередили про нове масове вимирання: Земля може втратити тисячі видів

09:26 Стало відомо, якої потужності буде магнітна буря 7 червня

LOAD MORE

### КАТЕГОРІЇ НОВИН

[Всі новини](#)

[Україна](#)

[Політика](#)

[Економіка](#)

[Світ](#)

[Стиль життя](#)

[Авто](#)

[Технології](#)

[Суспільство](#)

[Здоров'я](#)

### ІНФОРМАЦІЯ

[Про проект](#)

[Автори](#)

[Редакційна політика і стандарти](#)

[Політика використання ШІ](#)

[Політика конфіденційності](#)

[Правила коментування](#)

[Контакти](#)

ТОВ «НОВА МЕДІА ГРУПА» © 2014—2026

Реєстрація R40-06871 у Реєстрі суб'єктів у сфері медіа

Адреса: 01014, м. Київ, вул. Звіринська, 63

[editor@expert.in.ua](mailto:editor@expert.in.ua)

[corrections@expert.in.ua](mailto:corrections@expert.in.ua)

[reklama@expert.in.ua](mailto:reklama@expert.in.ua)