ASUS сообщила о критической уязвимости в роутерах с включённой функцией AiCloud, которая позволяет злоумышленникам удалённо выполнять несанкционированные действия. Уязвимость, обозначенная как CVE-2025-2492, получила оценку 9.2 по шкале CVSS, что указывает на её высокую опасность. Как сообщает The Hacker News, проблема связана с недостаточной проверкой аутентификации в прошивках ряда моделей роутеров. С помощью специально сформированного запроса хакеры могут получить контроль над устройством без ввода пароля.

AiCloud — это облачный сервис ASUS, превращающий роутер в мини-сервер для удалённого доступа к файлам на USB-накопителях, стриминга медиа и синхронизации данных. Уязвимость затрагивает прошивки серий 3.0.0.4_382, 3.0.0.4_386, 3.0.0.4_388 и 3.0.0.6_102. ASUS выпустила обновления прошивок для устранения проблемы и настоятельно рекомендует пользователям установить их через официальный сайт.

Для тех, кто не может обновить прошивку, например, на устаревших моделях, советуют отключить AiCloud. Также важно использовать сложные пароли длиной от 10 символов, включающие буквы, цифры и символы. Пока нет данных об активной эксплуатации уязвимости, но её потенциал для атак “требует немедленных действий”.