Что рекомендует пользователям компания, чтобы обезопасить свои устройства?

Компания ASUS (Asustek Computer Inc.) – это мировой производитель компьютерной техники и электроники, основанный в Тайване в 1989 году. Компания специализируется на производстве и продаже разнообразной продукции, включая ноутбуки, настольные компьютеры, мониторы, смартфоны, планшеты, компоненты для компьютеров (материнские платы, видеокарты, блоки питания и другие) и сетевое оборудование." data-html="true" data-original-title="Asus" >ASUS выпустила обновление прошивки, устраняющее уязвимость, которая затрагивает сразу семь моделей маршрутизаторов и позволяет удалённым злоумышленникам получить доступ к устройствам.

Критическая уязвимость, зарегистрированная как CVE-2024-3080 (оценка CVSS v3.1: 9.8) позволяет неавторизованным удалённым пользователям обходить аутентификацию и захватывать контроль над устройством.

Уязвимость затрагивает следующие модели маршрутизаторов ASUS:

ASUS рекомендует обновить прошивку вышеперечисленных маршрутизаторов до последней версии, доступной на портале загрузок компании. Инструкции по обновлению прошивки можно найти на странице FAQ.

Для тех, кто не может обновить прошивку немедленно, рекомендуется использовать надёжные пароли как для учётных записей, так и для самих Wi-Fi сетей — длиной более 10 символов. Также компания советует отключить доступ к административной панели через Интернет, удалённый доступ с WAN, переадресацию портов, DDNS, VPN сервер, DMZ и переключатель портов.

В том же пакете обновлений устранена уязвимость CVE-2024-3079, представляющая собой переполнение буфера (CVSS v3.1: 7.2), для эксплуатации которой требуется административный доступ.

Кроме того, CERT Тайваня сообщил об уязвимости CVE-2024-3912 (CVSS v3.1: 9.8), которая позволяет неавторизованным удалённым пользователям выполнять системные команды на устройстве. Эта уязвимость затрагивает множество моделей маршрутизаторов ASUS, но не все из них получат обновления безопасности из-за окончания срока поддержки.

Ниже перечислены решения по уязвимости CVE-2024-3912 для конкретных моделей

маршрутизаторов:

ASUS также выпустила обновление для фирменной утилиты Download Master, используемой для управления и загрузки файлов напрямую на подключённое к маршрутизатору USB-устройство через торренты, HTTP или FTP.

Новая версия Download Master 3.1.0.114 устраняет пять уязвимостей средней и высокой степени опасности, связанных с произвольной загрузкой файлов, внедрением команд ОС, переполнением буфера, отражённым и сохранённым XSS.

Хотя эти уязвимости не столь критичны, как CVE-2024-3080, пользователям рекомендуется обновить утилиту до версии 3.1.0.114 или выше для оптимальной безопасности.

На перекрестке науки и фантазии — наш канал