Компания Asus выпустила предупреждение для своих пользователей о серьёзной уязвимости, обнаруженной в маршрутизаторах бренда с поддержкой облачной функции AiCloud, позволяющей использовать такие роутеры как мини-серверы для обмена данными и доступа к файлам, которые размещены на подключённых USB-накопителях.

Выявленная уязвимость позволяет злоумышленникам обходить аутентификацию и выполнять команды удалённо. Отмечается, что уязвимость представляет собой значительный риск, поскольку может быть использована без необходимости авторизации. К тому же использование этой уязвимости может позволить злоумышленникам заразить устройства вредоносным ПО или организовать DDoS-атаки с помощью устройств пользователей.

Уязвимость затрагивает несколько моделей маршрутизаторов, что является следствием некорректного управления процессами аутентификации. Asus выпустила обновления прошивки для затронутых версий, включая версии 3.0.0.4_382, 3.0.0.4_386, 3.0.0.4_388 и 3.0.0.6_102, и настоятельно рекомендует пользователям обновиться до последней версии.

Для защиты беспроводной сети и панели управления маршрутизатора пользователям также рекомендуется устанавливать уникальные пароли длиной не менее 10 символов. Для устройств с истекшим сроком поддержки Asus рекомендует отключить функцию AiCloud и доступ к WAN, а также деактивировать различные функции: переадресацию портов, DDNS, VPN-серверы, DMZ и службы FTP.