**Уязвимость OpenWRT: киберэксперт Полунин о мерах предосторожности**

Специалист Flatt Security обнаружил критические уязвимости в системе обновления OpenWRT (Attended SysUpgrade — ASU), позволяющие злоумышленникам подменять легитимные образы прошивок вредоносными. Киберэксперт Сергей Полунин, руководитель группы защиты инфраструктурных ИТ-решений компании «Газинформсервис», подчеркнул необходимость превентивных мер для бизнеса для предотвращения подобных угроз безопасности.

Критическая уязвимость в функциональности ASU создаёт серьёзную киберугрозу для устройств, использующих OpenWRT. Она позволяет атакующим незаметно внедрять вредоносный код, получая полный контроль над скомпрометированными устройствами.

«*Подобные уязвимости довольно часто возникают, когда в процесс создания программного продукта вовлечено большое количество разработчиков, однако на постоянной основе отсутствуют необходимые инструменты для контроля безопасной разработки на каждом из этапов. Динамические и статические сканеры кода, всевозможные системы контроля зависимостей и подключаемых библиотек как раз решают эту задачу при правильной настройке и эксплуатации. Ну а если речь идёт о разработке крупных коммерческих приложений, то процесс разработки должен быть выстроен должным образом. Если требования к безопасности высоки, то необходимо подключать специалистов по тестированию на проникновение для крупных релизов, а также решения класса BAS, имитирующие действия злоумышленников», —* отметил **Сергей Полунин**.

**Справка о компании:**

[ООО «Газинформсервис»](https://www.gaz-is.ru/) — отечественный разработчик программных и программно-аппаратных средств обеспечения информационной безопасности и комплексной инженерно-технической охраны. Компания специализируется на создании систем обеспечения информационной безопасности объектов и ИБ-систем для корпораций энергетической и транспортной отраслей, органов государственной власти, промышленных предприятий, а также учреждений финансового сектора и телекоммуникационных компаний.