**Киберэксперт Полунин предупреждает: хакеры могут получить полный контроль над системой**

Обнаружена критическая уязвимость в широко используемой библиотеке libxml2, которая обрабатывает XML-данные в миллионах приложений и систем. Руководитель группы защиты инфраструктурных ИТ-решений компании «Газинформсервис» Сергей Полунин рекомендует использовать специализированные средства анализа безопасности и поведенческого анализа, такие как Ankey ASAP, чтобы выявить потенциальные уязвимости и аномалии в работе систем.

Уязвимость, классифицированная как CVE-2024-40896 (CVSS 9.1) и получившая критическую оценку серьёзности 9,1, позволяет злоумышленникам использовать атаки типа XXE (XML External Entities) для компрометации систем и кражи данных. Киберпреступники могут использовать уязвимость для выполнения вредоносного кода. Помимо кражи данных, это может дать злоумышленникам полный контроль над системой и спровоцировать отказ в обслуживании (DoS), исчерпав системные ресурсы.

*«Уязвимости класса XXE довольно редки и касаются программных продуктов, где используется XML. XML-процессор принимает какие-то данные в определённом формате и выдаёт результат. Проблемы начинаются, когда данные формируют таким образом, что заставляют XML-процессор сделать что-то, о чём не подумали разработчики, — прочитать системный файл, выполнить команду или даже повесить систему из-за бесконечного цикла операций. В этот раз уязвимость обнаружилась в крайне популярном libxml2, библиотеке, которая как раз и реализует работу в XML. При этом вы как разработчик можете и не знать, что эта библиотека используется в вашем продукте, если подключили её вместе с другими необходимыми для старта работы библиотеками. Даже при хорошо выстроенном процессе разработки программного обеспечения выявить такую уязвимость сложно. Однако есть продукты вроде Ankey ASAP, которые помогают выявить проблемы с ПО, даже если уязвимость ещё не опубликована. В ход идёт поведенческая аналитика и подобные механизмы. Для XML, безусловно, есть и альтернативы, но те тоже не лишены своих проблем»,* — 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.