**Взлом через NPM: как защититься от критической уязвимости?**

В популярном пакете Node.js Systeminformation обнаружена критическая уязвимость (RCE — удалённое выполнение кода), что ставит под угрозу безопасность систем, использующих эту библиотеку. Киберэксперт компании «Газинформсервис» Сергей Полунин рекомендует компаниям пересмотреть свои стратегии информационной безопасности и внедрить системы мониторинга безопасности, такие как Security Operations Center (SOC), для обнаружения угроз и реагирования на них в реальном времени.

*«Уязвимость в популярном NPM-пакете — это всегда серьёзная проблема. Дело в том, что сегодня почти ничего не пишется с нуля, а разработчики используют огромное количество сторонних библиотек и модулей, зачастую даже не задумываясь об их безопасности. Их тоже можно понять: их в большей степени интересует функционал. Поэтому, когда появляется информация об уязвимости, особенно класса RCE, в библиотеке, которую вы используете, то это повод задуматься о том, как вы вообще проектируете своё программное обеспечение. Я не говорю, что всё нужно делать самому. Это как раз, скорее всего, сделает ваше ПО ещё более уязвимым, а вот использовать наложенные средства при тестировании и развёртывании ваших приложений — это хорошая идея. Подключив своё приложение к тому же SOC, выявлять атаки на эксплуатацию уязвимостей будет довольно просто. А ещё правильнее не допускать их в принципе. Для этого существует методология DevSecOps, которая позволяет на каждом этапе разработки ПО контролировать различные аспекты безопасности»,* — комментирует руководитель группы защиты инфраструктурных ИТ-решений компании «Газинформсервис» **Сергей Полунин**.

Напомним, в мае этого года «Газинформсервис» запустил коммерческий SOC, предоставляющий круглосуточный мониторинг и реагирование на инциденты безопасности. В основе решения лежат SIEM-, VM-, XDR- и UEBA-системы, позволяющие эффективно выявлять и нейтрализовывать угрозы, подобные внедрению команд в популярном пакете NPM Systeminformation. Состав решения может быть адаптирован под потребности конкретного заказчика.

**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.