**Эксперт Дмитриева: 100 000 сайтов WordPress под угрозой из-за уязвимости в плагине SureTriggers**

SureTriggers, популярный плагин WordPress, содержит критическую уязвимость, позволяющую злоумышленникам создавать учётные записи администраторов. Под угрозой находятся более 100 000 сайтов с устаревшими версиями плагина. Уже зафиксированы атаки на уязвимые сайты.

Инженер-аналитик лаборатории исследований кибербезопасности компании «Газинформсервис» Ирина Дмитриева объясняет: *«Публикация информации об уязвимости в плагине WordPress SureTriggers привела к первым кибератакам на CMS, доступным в сети. Успешная атака на сервис стала возможна из-за недостаточной проверки заголовка ST-Authorization в REST API плагина SureTriggers в версиях младше 1.0.78. Обойти аутентификацию можно после отправки некорректного заголовка».*

Уязвимость позволяет хакерам обеспечить закрепление через легитимные учётные записи администраторов для последующего внедрения вредоносного кода, кражи данных или фишинга.

*«Рекомендуется провести незамедлительное обновление плагина до версии 1.0.78, в которой устранена уязвимость. До тех пор можно временно деактивировать плагин. При проверке нелегитимной активности важно проверить журналы доступа на аномальные запросы с IP-адресов, не связанных с легитимной активностью, а также провести аудит учётных записей и плагинов. Для проактивной защиты важно внедрить автоматическое сканирование уязвимостей. Например, OWASP ZAP подходит для тестирования REST API на корректность проверки заголовков авторизации. Комплексно детектировать атаки на веб-сегменты инфраструктуры возможно при наличии SIEM, которые позволяют централизованно мониторить попытки создания/изменения учётных записей администраторов. Отмечу, что система мониторинга Ankey SIEM NG от компании "Газинформсервис" позволяет обеспечить комплексный мониторинг информационной безопасности всей инфраструктуры компании, в частности, наглядность атаки будет отражена у аналитика безопасности в панели мониторинга»,* — отмечает **Дмитриева**.

**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.