**Бронированный Linux: киберэксперт о том, как защититься от взлома ядра**

В сети появились готовые инструменты (эксплойты) для атаки на критические уязвимости CVE-2024-56614 и CVE-2024-56615 в ядре Linux, позволяющие злоумышленникам получить полный контроль над системой. Инженер-аналитик компании «Газинформсервис» Александр Катасонов предупреждает, что это представляет серьёзную угрозу безопасности для миллионов пользователей Linux по всему миру, так как хакеры теперь могут легко использовать эти уязвимости для компрометации систем.

Уязвимости CVE-2024-56614 и CVE-2024-56615, связанные с eBPF (Extended Berkeley Packet Filter), позволяют злоумышленникам получить возможность управлять операционной системой от имени администратора (root-доступ) и установить вредоносное ПО.

Угроза реальна и масштабна: уязвимости влияют на обработку пакетов с помощью сокетов AF\_XDP, а опубликованные эксплойты существенно повышают риск атак.

«*Уязвимости, связанные с ядром операционной системы, являются одними из самых опасных с точки зрения безопасности, поскольку их эксплуатация может позволить злоумышленнику получить права, превышающие привилегии root. Подобные атаки нередко используются для скрытой установки руткитов, которые могут долгое время оставаться незамеченными и обеспечивать полный контроль над системой. Для защиты компании необходимо использовать средства информационной безопасности, такие как Efros Defence Operations. В современных условиях недостаточно просто обновлять ядро операционной системы, необходимо контролировать всю инфраструктуру в реальном времени. Решения уровня Efros DefOps способны обнаруживать изменения в инфраструктуре, оперативно уведомлять о них и обеспечивать экстренное реагирование на инциденты*», — отметил **Александр Катасонов**, инженер-аналитик лаборатории развития и продвижения компетенций кибербезопасности компании «Газинформсервис».

**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.