НКЦКИ
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

Угроза несанкционированного доступа к данным различных организаций

ALRT-20230608.2 | 8 июня 2023 г.

Уровень угрозы: КРИТИЧЕСКИЙ

TLP: WHITE

Описание угрозы	По каналам НКЦКИ получены сведения об используемом злоумышленниками методе получения несанкционированного доступа к конфиденциальным данным различных организаций Российской Федерации. Злоумышленники прилагают усилия к получению конфиденциальных сведений из списанного, отданного в ремонт, реализованного на вторичном рынке сетевого и серверного оборудования, а также пользовательских устройств производственных и технологических компаний, разработчиков программного обеспечения, центров облачных вычислений и обработки информации. При удачном восстановлении или получении неудалённых с устройств сведений злоумышленники продают их на специализированных торговых площадках теневого сегмента сети «Интернет» или используют в целенаправленных атаках на организацию. К таким сведениям относятся: – информация о клиентах, партнерах и смежных предприятиях; – сертификаты безопасности, криптографические токены и ключи; – сведения о об используемых в организации программах и платформах; – сведения о настройках портов и хостов, через которые производилось взаимодействия с внешними сетями; – учетные записи администраторов, настройки VPN и IPSEC; – и иные конфиденциальные данные организации.
Рекомендации по нейтрализации угрозы	– разработать внутренний порядок списания оборудования, предусматривающий выполнение требований по защите информации при утилизации, передаче в ремонт или реализации оборудования на вторичном рынке; – необходимо следовать рекомендациям производителей оборудования по очистке памяти (форматированию) при продаже, списании и ремонте; – использовать съемные носители для хранения файлов конфигурации; – регулярно проводить централизованную смену криптографических ключей; – механически разрушать или оставлять на хранение электронные носители информации в случае выхода оборудования или устройства из строя перед его утилизацией.