Компания спешно выпускает заплатки, исправляя в сумме 16 уязвимостей.

21 мая компания Ivanti – американская компания, специализирующаяся на разработке программного обеспечения для управления информационными технологиями. Компания была основана в 1985 году под именем LANDESK, а затем переименована в Ivanti в 2017 году.

 Ivanti предоставляет широкий спектр решений для автоматизации и оптимизации процессов IT-управления в компаниях и организациях. Продукты компании включают инструменты для управления конечными точками (например, компьютерами и мобильными устройствами), управления сервисными запросами, управления обновлениями и безопасностью, а также инструменты для автоматизации работы IT-специалистов." data-html="true" data-original-title="Ivanti" >Ivanti выпустила обновления для устранения множества критических уязвимостей в таких продуктах, как Endpoint Manager, Avalanche – это открытая платформа для создания и запуска децентрализованных приложений, смарт-контрактов и кастомных блокчейнов в единой масштабируемой экосистеме. Блокчейн Avalanche состоит из трех основных цепей: X-Chain, C-Chain и P-Chain, которые обеспечивают интероперабельность, гибкость и безопасность.

 Блокчейн Avalanche использует новый алгоритм консенсуса, основанный на семействе протоколов Snow, который позволяет достигать высокой пропускной способности, низкой задержки и надежной финальности. Avalanche также поддерживает создание подсетей, которые являются независимыми, но связанными блокчейнами, валидируемыми динамическими подмножествами валидаторов. Блокчейн имеет собственный токен AVAX, который используется для оплаты комиссий, участия в стейкинге и управлении сетью." data-html="true" data-original-title="Avalanche" >Avalanche, Neurons for ITSM, Ivanti Connect Secure – это решение для обеспечения безопасного удалённого доступа, которое используется организациями для предоставления своим сотрудникам возможности безопасного подключения к корпоративной сети с любого устройства, в любое время и из любого места. Эта система включает в себя различные функции безопасности, такие как аутентификация, шифрование данных и защита от различных видов киберугроз, обеспечивая надёжный доступ к корпоративным ресурсам и приложениям через Интернет." data-html="true" data-original-title="Connect Secure" >Connect Secure и Secure Access. Суммарно было исправлено 16 уязвимостей, которые мы кратко рассмотрим ниже.

Из десяти выявленных уязвимостей в Endpoint Manager шесть связаны с SQL-инъекциями (CVE-2024-29822, CVE-2024-29823, CVE-2024-29824, CVE-2024-29825, CVE-2024-29826, CVE-2024-29827). Они имеют оценку 9.6 по шкале CVSS. Эти уязвимости позволяют неаутентифицированному злоумышленнику, находящемуся в

той же сети, выполнить произвольный код.

Остальные четыре уязвимости в Endpoint Manager (CVE-2024-29828, CVE-2024-29829, CVE-2024-29830, CVE-2024-29846) уже требуют аутентификации атакующего, но также позволяют выполнить произвольный код. Эти недостатки имеют оценку 8.4 по шкале CVSS, затрагивая Core сервер Ivanti EPM 2022 SU5 и более ранние версии.

В клиенте Ivanti Avalanche версии 6.4.3.602 компания исправила критическую уязвимость CVE-2024-29848 (CVSS 7.2), позволяющую хакерам удалённо выполнять код через загрузку специально созданного файла.

Также компания выпустила патчи для пяти других уязвимостей высокой степени опасности: SQL-инъекция (CVE-2024-22059, CVSS 8.8) и ошибка неограниченной загрузки файлов (CVE-2024-22060, CVSS 8.7) в Ivanti Neurons for ITSM, CRLF-инъекция в Ivanti Connect Secure (CVE-2023-38551, CVSS 8.2) и две уязвимости локального повышения привилегий в Ivanti Secure Access: CVE-2023-38042, CVSS 7.8 (затрагивает Windows) и CVE-2023-46810, CVSS 7.3 (затрагивает Linux).

Компания подчеркнула, что у неё нет доказательств эксплуатации всех этих уязвимостей в реальных атаках или их внедрения в процесс разработки кода через цепочку поставок.

Клиентам Ivanti рекомендуется незамедлительно установить последние исправления безопасности для устранения критических уязвимостей. Также крайне важно регулярно проверять наличие обновлений, следовать лучшим практикам кибербезопасности, проводить аудит систем и процессов, а также иметь план реагирования на инциденты для быстрой реакции в случае настоящего взлома.