Обновитесь до последней версии, чтобы не стать очередной жертвой кибербандитов.

Американская компания SolarWinds, специализирующаяся на разработке программного обеспечения для управления IT-инфраструктурой, объявила о выпуске обновлений безопасности, направленных на устранение нескольких критических уязвимостей в своих продуктах Serv-U, а также платформе SolarWinds. Эти уязвимости затрагивают версию 2024.1 SR 1 и предыдущие версии.

Об одной из уязвимостей, получившей обозначение CVE-2024-28996, сообщил Нилс Путнинс, специалист по тестированию на проникновение, работающий в Агентстве связи и информации НАТО. Уязвимость получила оценку CVSS (Common Vulnerability Scoring System) — это открытый стандарт, используемый для оценки и классификации уязвимостей информационной безопасности. CVSS предоставляет числовую оценку, которая помогает организациям определить серьезность уязвимости и принять соответствующие меры для устранения угроз.

 Оценка CVSS представлена числовым значением от 0 до 10, где 0 обозначает отсутствие уязвимости, а 10 — наивысший уровень уязвимости. Эта оценка позволяет IT-специалистам и администраторам принимать решения о приоритетах по обеспечению безопасности систем и принимать меры для устранения уязвимостей, наиболее критичных для организации." data-html="true" data-original-title="CVSS" >CVSS 7.5 и заключается в доступном только для чтения подмножестве SQL, SWQL, которое позволяет пользователям запрашивать информацию о сети в базе данных SolarWinds

Согласно опубликованному консультативному документу, сложность атаки оценивается как «высокая», что несколько обнадёживает, ограничивая использование уязвимости только высококвалифицированными хакерами.

Помимо CVE-2024-28996, специалисты SolarWinds устранили и несколько других уязвимостей в своей платформе. Так, уязвимость CVE-2024-28999 (CVSS 6.4) является проблемой типа Race Condition, а CVE-2024-29004 (CVSS 7.1) — XSS-уязвимостью в веб-консоли.

Компания также исправила ряд ошибок в сторонних компонентах, включая Angular (CVE-2021-4321), публичную API-функцию «BIO_new_NDEF» (CVE-2023-0215), алгоритм генерации ключей RSA в OpenSSL (CVE-2018-0737), процедуру возведения в квадрат Монтгомери для x86_64 в OpenSSL (CVE-2017-3736) и множество других уязвимостей.

На данный момент неизвестно, использовались ли все эти уязвимости в реальных атаках, однако, чтобы не узнать этого на собственном горьком опыте, рекомендуется

как можно быстрее совершить обновление до версии SolarWinds 2024.2, которая устраняет все вышеуказанные уязвимости.