CVE-2024-3094 наконец-то устранили в версии 5.6.2.

Ровно два месяца назад киберпространство содрогнулось от выпуска срочного предупреждения, касающегося вредоносного кода в XZ Utils, который оказался бэкдором, добавленным злоумышленником под псевдонимом Цзя Тан. Предположительно китайский хакер, или даже целая группа хакеров, сумела расположить к себе пользователей и стать со-разработчиком проекта.

Лишь спустя два месяца ведущий разработчик XZ Лассе Коллин наконец выпустил версию XZ 5.6.2 с полностью удалённым бэкдором.

XZ Utils — это кроссплатформенный набор программ для сжатия данных. Они используются преимущественно в Linux для уменьшения размера файлов, что помогает экономить место на диске и ускорять передачу данных по сети. Основным компонентом XZ Utils является библиотека liblzma, которая обеспечивает алгоритм сжатия данных LZMA.

Уязвимость CVE-2024-3094, которая присутствовала в предыдущих версиях 5.6 и 5.6.1., была полностью устранена в свежем релизе. Тем временем, расследование ситуации с бэкдором продолжается, а все желающие могут следить за обновлениями на специальной странице XZ.

Также Лассе Коллин сообщил, что злополучного Цзя Тана в роли поддерживающего разработчика XZ заменит Сэм Джеймс.

Помимо удаления Бэкдор (от англ. «backdoor», что буквально переводится как «задняя дверь») — это техническое средство, позволяющее обойти стандартные процедуры аутентификации или другие защитные механизмы в системе, программе или устройстве. С помощью бэкдора злоумышленники могут получить несанкционированный доступ к ресурсам системы или управлять ею.

 Бэкдоры могут быть внедрены в программное обеспечение как на этапе его разработки, так и уже в ходе его эксплуатации (например, через вредоносное ПО). Они могут быть использованы как для шпионажа, так и для удаленного управления системой или устройством." data-html="true" data-original-title="Бэкдор" >бэкдора, в XZ 5.6.2 были исправлены несколько багов, добавлена поддержка компилятора NVIDIA HPC SDK и убрана поддержка GNU Indirect Function (IFUNC). IFUNC использовался в бэкдоре, но его удаление было обусловлено тем, что его преимущества для производительности были незначительными, а сложность кода существенно возрастала.

Кроме XZ 5.6.2 также были выпущены версии XZ 5.4.7 и XZ 5.2.13, содержащие различные исправления ошибок. Однако только версия XZ 5.6 была подвержена проблеме с внедрённым бэкдором.