AIRNITE

ZERO DAY

ВЫПУСК 03/2026 · ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

На полсекунды медленнее: как бэкдор xz едва не попал в Linux

В марте 2024 года разработчик заметил, что вход по SSH занимает чуть больше времени, чем нужно, — и обнаружил бэкдор в утилите сжатия xz. Что произошло и какие выводы компании могут сделать для своего ПО.

Опубликовано: 21 ноября 2026 г. Время чтения: 6 мин Автор: Редакция Airnite

SOFTWARE. SECURITY. CODE.

// СИТУАЦИЯ В ЦИФРАХ

5.6.0 / 5.6.1
уязвимые версии xz
по данным первооткрывателя, Red Hat и CISA

0,3 → 0,8 с
замедление входа по SSH
измерение первооткрывателя Андреса Фройнда (oss-security)

29.03.2024
публикация и предупреждение CISA
в один и тот же день (oss-security, CISA)

5.4.6
рекомендуемая версия для отката
пример незатронутой версии, по данным CISA

В конце марта 2024 года разработчик Андрес Фройнд обратил внимание на мелочь: вход по SSH на его тестовых системах с Debian «sid» потреблял подозрительно много процессорного времени, а вдобавок инструмент проверки сообщал об ошибках. Вместо того чтобы отмахнуться, он стал разбираться. 29 марта 2024 года он опубликовал результат: широко распространённая утилита сжатия **xz** содержала бэкдор, нацеленный на SSH-серверы.

// Что произошло?

Фройнд написал в рассылке oss-security, что в upstream-репозиторий xz и опубликованные релизные архивы был встроен бэкдор. Уязвимыми оказались версии **5.6.0 и 5.6.1**. Red Hat присвоила уязвимости идентификатор **CVE-2024-3094**; компания Rapid7, специализирующаяся на безопасности, сообщает о максимальной оценке CVSS 10. В тот же день американское ведомство CISA выпустило предупреждение и рекомендовало откатиться на незатронутую версию, например **5.4.6**.

Red Hat призвала пользователей Fedora Rawhide немедленно прекратить использование этих систем, а затронутых пользователей Fedora 40 — вернуться на xz 5.4; Red Hat Enterprise Linux затронута не была. Сам Фройнд писал, что новые версии ещё почти не успели попасть в дистрибутивы. Иными словами, бэкдор обнаружили незадолго до того, как он оказался бы в крупных стабильных выпусках Linux.

// Как устроена атака?

Изощрённость в том, что ключевая часть, по словам Фройнда, содержалась **только в распространяемых релизных архивах**, а не в общедоступном исходном коде. Изменённый сценарий сборки при сборке пакета внедрял вредоносный код в библиотеку liblzma. Тот, кто проверял лишь исходный код в репозитории, ничего подозрительного не видел.

До SSH-сервера код добирался обходным путём: ряд дистрибутивов дополняет OpenSSH интеграцией с systemd, а используемая для этого библиотека, в свою очередь, загружает liblzma. По словам Фройнда, вредоносный код активировался только при определённых условиях, в том числе на Linux x86-64 и при сборке в виде пакета Debian или RPM. По его измерениям, время входа по SSH выросло с 0,3 до 0,8 секунды — достаточно, чтобы это заметить.

Кто за этим стоит, неизвестно. Фройнд писал, что автор коммитов либо был причастен напрямую, либо его система была серьёзно скомпрометирована. Отраслевые издания, такие как Dark Reading, описывают годами готовившееся внедрение в проект, в ходе которого целенаправленно завоёвывалось доверие сообщества разработчиков.

// Кого это касается?

Непосредственно затронуты были прежде всего тестовые и предварительные версии дистрибутивов Linux, например Debian «sid» и Fedora Rawhide. Но реальное значение случая гораздо шире: xz — маленькая, незаметная утилита, которая работает во множестве систем Linux. Если ломается такое звено **цепочки поставок ПО**, под угрозой потенциально оказываются серверы по всему миру, хотя их администраторы ничего сознательно не устанавливали.

Для компаний это означает: даже те, кто не разрабатывает собственное ПО, зависят от компонентов с открытым исходным кодом, которые часто поддерживает горстка добровольцев. Кто не знает, какие версии работают в его системах, не сможет быстро отреагировать в критической ситуации.

// Что делать сейчас?

Неотложные меры 2024 года давно приняты. Неизменным остаётся урок: компаниям нужен актуальный обзор своих компонентов, отработанный порядок действий при предупреждениях о безопасности и чёткое разделение тестовых и рабочих систем. И к аномалиям нужно относиться серьёзно — бэкдор в xz нашли потому, что кто-то не проигнорировал задержку в полсекунды. Чек-лист ниже сводит шаги воедино.

// Чем поможет Airnite?

Airnite создаёт **программное обеспечение** с прослеживаемой цепочкой поставок и составляет перечни компонентов для существующих систем. В ходе **тестирования на проникновение** мы проверяем серверы и среды сборки на наличие устаревших и уязвимых компонентов. В рамках **консалтинга** мы вместе с вами выстраиваем процесс, который оценивает предупреждения, находит затронутые системы и управляет обновлениями.

> Примечание: обзорная статья об инциденте 2024 года. Данные актуальны на 21 ноября 2026 года.

Чек-лист: что сделать прямо сейчас

[+] Вести перечень компонентов (SBOM) для всех собственных и используемых систем, чтобы уязвимые версии можно было найти немедленно.

[+] Подписаться на предупреждения о безопасности от CISA, BSI и дистрибутивов и назначить ответственного за их оценку.

[+] Отделить тестовые системы и системы разработки с предварительными версиями (например, rolling-релизами) от рабочей сети и от учётных данных.

[+] Собирать ПО из прослеживаемых источников и, где возможно, проверять воспроизводимость сборок; сравнивать релизные архивы с состоянием исходного кода.

[+] Относиться к аномалиям серьёзно: необъяснимую нагрузку или задержки в работе сервисов вроде SSH расследовать, а не списывать на случайность.

[+] Поддерживать критически важные проекты с открытым исходным кодом, на которые опирается ваш бизнес, — деньгами, ресурсами на аудит или участием в разработке.

Чем поможет Airnite

- Разработка и сайты – Сайты и веб-приложения: быстрые, безопасные, многоязычные.
- Пентест и безопасность – Контролируемые атаки с понятным отчётом и планом мер.
- Консалтинг – Взгляд со стороны на ваши планы и проекты.

Знаете ли вы, из чего состоит ваше ПО?

Airnite вместе с вами составляет обзор всех компонентов с открытым исходным кодом в ваших системах (SBOM), проверяет процессы сборки на возможность манипуляций и настраивает оповещения о критических уязвимостях. Так в следующий раз вы отреагируете за часы, а не за недели.

Запросить первичную консультацию · Написать на эл. почту · Через WhatsApp

Контакты

Есть вопросы по статье? Напишите нам в WhatsApp: +49 174 6834842

Читать онлайн: https://airnite.de/ru/zhurnal/bekdor-xz-utils-linux/

Источники

Каждый факт в этой статье подтверждён следующими источниками. Первоисточники отмечены.

1. **oss-security · Andres Freund: backdoor in upstream xz/liblzma leading to ssh server compromise** · 29 марта 2024 г. · ПЕРВОИСТОЧНИК
   Первоисточник: обнаружение, уязвимые версии, механизм только в релизных архивах, условия срабатывания
   https://www.openwall.com/lists/oss-security/2024/03/29/4

2. **CISA · Reported Supply Chain Compromise Affecting XZ Utils Data Compression Library, CVE-2024-3094** · 29 марта 2024 г. · ПЕРВОИСТОЧНИК
   Предупреждение ведомства США: уязвимые версии, рекомендация откатиться, например, на 5.4.6
   https://www.cisa.gov/news-events/alerts/2024/03/29/reported-supply-chain-compromise-affecting-xz-utils-data-compression-library-cve-2024-3094

3. **Red Hat · Urgent security alert for Fedora Linux 40 and Fedora Rawhide users** · 29 марта 2024 г., обновлено 30 марта 2024 г. · **ПЕРВОИСТОЧНИК**
   Предупреждение производителя: Fedora Rawhide и бета-версия Fedora 40, RHEL не затронута
   https://www.redhat.com/en/blog/urgent-security-alert-fedora-41-and-rawhide-users

4. **Rapid7 · Backdoored XZ Utils (CVE-2024-3094)** · 1 апреля 2024 г.
   Исследование безопасности: оценка, рейтинг CVSS 10
   https://www.rapid7.com/blog/post/2024/04/01/etr-backdoored-xz-utils-cve-2024-3094/

5. **Dark Reading · XZ Utils Backdoor Implanted in Carefully Executed, Multiyear Supply Chain Attack** · 2024
   Отраслевые СМИ: внедрение в проект, готовившееся годами
   https://www.darkreading.com/cyber-risk/xz-utils-backdoor-implanted-in-intricate-multi-year-supply-chain-attack

Общая редакционная информация, а не юридическая консультация и не индивидуальная проверка ваших систем. Актуально на дату публикации.

Airnite GmbH · Am Waldbach 7 · 77654 Offenburg · airnite.de