Рекомендации по безопасности LFS

LFS 12.1 и текущие книги по разработке.

LFS-12.1 был выпущен 1 марта 2024 г.

- В настоящее время нет известных уязвимостей безопасности для LFS-12.1.

На этой странице пакеты расположены в алфавитном порядке, и если пакет содержит несколько рекомендаций, сначала появляются новые.

Ссылки в конце каждого пункта ведут к более подробной информации, содержащей ссылки на книги по разработке.

Expat

12.1 010 Expat (LFS) Дата: 2024-03-20 Серьезность: Средняя

В Expat-2.6.2 была исправлена уязвимость безопасности, которая могла допустить отказ в обслуживании через атаку XML Entity Expansion при изолированном использовании внешних парсеров (созданных с помощью функции XML_ExternalEntityParserCreate). Проблема была классифицирована как атака «миллиард смеха», также известная как атака XML-бомбы. Этой уязвимости был присвоен номер CVE-2024-28757.

Чтобы устранить эту уязвимость, обновите Expat-2.6.2, используя инструкции для Expat (sysv) или Expat (systemd) . Примечание. Если вы установили docbook-utils из BLFS, вам нужно будет добавить «–without-docbook», чтобы обойти ошибку в настройке, поскольку наша установка docbook-utils использует SGML вместо XML.

Glibc

12.1 037 Glibc (LFS) Дата: 2 мая 2024 г. (обновлено 13 мая 2024 г.) Уровень серьезности: высокий.

В модуле iconv Glibc-2.39 и более ранних версий была обнаружена уязвимость безопасности, которая может позволить удаленное выполнение кода через сетевые службы, работающие в системе (был продемонстрирован эксплойт через веб-приложения на основе PHP). А в демоне кэша службы имен, или NSCD Glibc, были обнаружены четыре уязвимости, которые могут, по крайней мере, привести к отказу в обслуживании. NSCD отключен в сборке Glibc начиная с LFS 12.1, но в более ранних выпусках LFS все еще может использоваться уязвимый NSCD. Уязвимости iconv присвоен CVE-2024-2961, а уязвимостям NSCD присвоены CVE-2024-33599, CVE-2024-33600, CVE-2024-33601 и CVE-2024-33602.

Чтобы исправить уязвимость iconv, обновитесь до Glibc-2.39 или новее, используя инструкции из книги LFS для Glibc (sysv) или Glibc (systemd) , но после применения примените еще один патчglibc-2.39-fhs-1.patch . Чтобы безопасно обновить Glibc с версии 2.38 или более ранней до версии 2.39 в работающей системе, необходимы некоторые дополнительные меры предосторожности, как описано в поле «Важно» в разделе книги по Glibc. Следуйте этому

строго, иначе вы можете сделать систему полностью непригодной для использования. ВЫ ПРЕДУПРЕЖДЕНЫ. Для LFS 12.0 и более ранних версий процесс обновления также отключит и удалит NSCD, чтобы избавиться от уязвимостей NSCD.

Linux Kernel

12.1 029 Ядро Linux (LFS) Дата: 17 апреля 2024 г. Уровень серьезности: средний

В Linux-5.16.14 были добавлены обходные пути для уязвимостей оборудования под названием Branch History Injection. Эти уязвимости могут быть использованы для утечки конфиденциальной информации. Подробности читайте в статье. Уязвимости были присвоены номера CVE-2022-0001 и CVE-2022-0002 (для x86), а также CVE-2022-23690 (для ARM, пока не разглашается).

Чтобы обойти их, обновите Linux-5.16.14 (или 5.15.28, 5.10.105, 5.4.184, 4.19.234, 4.14.271, 4.9.306 для более старых систем, использующих стабильные ядра LTS), используя инструкции. из книги LFS для ядра Linux (sysv) или ядра Linux (systemd) и отключите непривилегированный системный вызов BPF с помощью параметра конфигурации ядра BPF_UNPRIV_DEFAULT_OFF=уили sysctl kernel.unprivileged_bpf_disabled=2.

Это обновление безопасности может оказать влияние на производительность, особенно на процессорах AMD, однако тесты от редакторов LFS показывают, что влияние незначительно.