

Переполнение буфера в MDAemon IMAP Server

Программа: MDAemon 9.6.4, возможно, более ранние версии.

Опасность: Средняя.

Описание: Уязвимость существует из-за ошибки проверки границ данных в IMAP-сервере при обработке команды FETCH. Удаленный пользователь может с помощью специально сформированной команды FETCH, содержащей слишком длинную спецификацию секции в элементе BODY, вызвать переполнение стека и выполнить произвольный код на целевой системе.

URL производителя: www.altn.com/products/default.asp/product_id/MDaemon.

Решение: В настоящее время способов устранения уязвимости не существует.

Уязвимость в утилите eMBox в Novell eDirectory

Программа: Novell eDirectory 8.8 и более ранние версии; Novell eDirectory 8.7.3.9 и более ранние версии.

Опасность: Низкая.

Описание: Уязвимость существует из-за неизвестной ошибки в утилите eMBox. Удаленный пользователь может получить доступ к некоторым файлам или вызвать отказ в обслуживании.

URL производителя: www.novell.com/products/edirectory.

Решение: Установите последнюю версию 8.8.2 с сайта производителя.

Множественные уязвимости в VMware Workstation

Программа: VMware Workstation версии до 6.0.3.

Опасность: Низкая.

Описание: 1. Уязвимость существует из-за ошибки в authd. Локальный пользователь может повысить свои привилегии на системе.

2. Уязвимость существует из-за ошибки в OpenSSL. Удаленный пользователь может вызвать отказ в обслуживании.

URL производителя: www.vmware.com/products/ws.

Решение: Установите последнюю версию 6.0.3 с сайта производителя.

Раскрытие данных в Gentoo Linux

Программа: Gentoo Linux 1.x.

Опасность: Низкая.

Описание: Уязвимость существует из-за того, что ebuilds вызывает функцию docert() из ssl-cert eclass в момент компиляции пакета из исходного кода. Это приводит к тому, что важные SSL-сертификаты включаются в генерируемый пакет, что может позволить злоумышленнику извлечь ключи для последующих атак. Для успешной эксплуатации уязвимости требуется, чтобы бинарный пакет был собран с опциями «--buildpkg» или «--buildpkgonly».

URL производителя: www.gentoo.org.

Решение: Установите последнюю версию с сайта производителя.

Несколько уязвимостей в MaxDB

Программа: MaxDB 7.6.0.37, возможно, более ранние версии.

Опасность: Средняя.

Описание: 1. Уязвимость существует из-за ошибки проверки знаковых переменных в компоненте vserver. Удаленный пользователь может отправить специально сформированный пакет на порт приложения 7210/TCP, вызвать повреждение динамической памяти и выполнить произвольный код на целевой системе. Для успешной эксплуатации уязвимости злоумышленник должен знать имя локальной базы данных.

2. Уязвимость существует из-за ошибки в приложении «sdbstarter» при обработке переменных окружения. Локальный пользователь, член группы sdba, может повысить свои привилегии на системе.

URL производителя: www.mysql.com/products/maxdb.

Решение: В настоящее время способов устранения уязвимости не существует.

Множественные уязвимости в VMware Server

Программа: VMware Server версии до 1.0.5.

Опасность: Низкая.

Описание: 1. Уязвимость существует из-за неизвестной ошибки в authd. Злоумышленник может заставить процесс authd подключиться к именованному каналу, который контролируется злоумышленником, и повысить свои привилегии на системе.

2. Уязвимость существует из-за неизвестной ошибки при обработке небезопасным образом созданных объектов именованных каналов. Злоумышленник может вызвать отказ в обслуживании или повысить свои привилегии на системе.

3. Две уязвимости существуют из-за небезопасных привилегий на доступ к файлу config.ini. Злоумышленник может повысить свои привилегии на системе.

4. Уязвимость существует из-за ошибки в OpenSSL. Злоумышленник может обойти некоторые ограничения безопасности на системе.

URL производителя: www.vmware.com/products/server.

Решение: Установите последнюю версию 1.0.5 с сайта производителя.

Раскрытие данных в OpenSSH

Программа: OpenSSH 4.7p1 и более ранние версии.

Опасность: Низкая.

Описание: Уязвимость существует из-за того, что sshd некорректно открывает TCP-порты на локальном IPV6-интерфейсе, если требуемые порты на IPV4-интерфейсе используются. Локальный пользователь может перехватить перенаправленную X11-сессию путем слушания на порту, используемом sshd для перенаправления локального X11-дисплея (например, порт 6010/TCP).

URL производителя: openssh.com.

Решение: В настоящее время способов устранения уязвимости не существует.

Составил Александр Антипов