

Отказ в обслуживании в OpenSSL

Программа: OpenSSL версии 0.9.8f и 0.9.8g.

Опасность: Средняя.

Описание: 1. Уязвимость существует из-за ошибки двойного освобождения памяти при обработке данных расширения имени сервера. Удаленный пользователь может вызвать отказ в обслуживании приложения, использующего OpenSSL. Для успешной эксплуатации уязвимости OpenSSL должен быть собран с использованием TLS-расширений имени сервера.

2. Уязвимость существует из-за неизвестной ошибки, которая позволяет удаленному пользователю, контролирующему злонамеренный сервер, вызвать отказ в обслуживании клиентского приложения, использующего OpenSSL, когда «Server Key exchange message» не участвует в клиентском TLS-рукопожатии.

URL производителя: www.openssl.org.

Решение: Установите последнюю версию 0.9.8h с сайта производителя.

Обход ограничений безопасности в Skype

Программа: Skype 3.6.0.248, возможно, более ранние версии.

Опасность: Средняя.

Описание: Уязвимость существует из-за ошибки проверки расширений файлов в «file:» URI-обработчике. Удаленный пользователь может изменить регистр в расширении файла или указать файл, который не содержится в списке опасных файлов (список состоит из следующих расширений: .ade, .adp, .asd, .bas, .bat, .cab, .chm, .cmd, .com, .cpl, .crt, .dll, .eml, .exe, .hlp, .hta, .inf, .ins, .isp, .js), это приведет к тому, что приложение не отобразит окно предупреждения об опасном типе файла.

URL производителя: www.skype.com.

Решение: Установите последнюю версию 3.8.0.139 с сайта производителя.

Множественные уязвимости в IBM DB2

Программа: IBM DB2 9.1.

Опасность: Средняя.

Описание: 1. Уязвимость существует из-за неизвестной ошибки в плагинах разработки CLR-храняемых процедур в Visual Studio.

2. Уязвимость существует из-за ошибки проверки границ данных в функции SQLRLAKA(). Удаленный пользователь может вызвать переполнение стека.

3. Уязвимость существует из-за неизвестной ошибки, связанной с созданием файлов на административном сервере. Локальный пользователь может повысить свои привилегии на системе.

4. Уязвимость существует из-за ошибок проверки границ данных в XQUERY, XMLQUERY, XMLEXISTS и XMLTABLE. Удаленный пользователь может вызвать переполнение буфера.

URL производителя: www-306.ibm.com/software/data/db2/9.

Решение: Установите исправление с сайта производителя.

Обход ограничений безопасности в Snort

Программа: Snort версии до 2.8.1.

Опасность: Средняя.

Описание: Уязвимость существует из-за ошибки дизайна при обработке фрагментированных IP-пакетов. Когда Snort получает фрагментированный пакет, осуществляется проверка значения Time To Live (TTL) и сравнение его со значением начального фрагмента. Если разница между значениями TTL-фрагментов больше, чем сконфигурировано (максимальное значение 5), фрагмент будет проигнорирован. Удаленный пользователь может с помощью фрагментированных валидных IP-пакетов обойти все правила фильтрации Snort.

URL производителя: www.snort.org.

Решение: Установите последнюю версию 2.8.1 с сайта производителя.

Утечка памяти в vsftpd в Red Hat Linux

Программа: Fedora 7, 8, 9; Red Hat Enterprise Linux (v. 5 server); Red Hat Enterprise Linux Desktop Workstation (v. 5 client); rPath Linux 1.x.

Опасность: Средняя.

Описание: Уязвимость существует из-за ошибки в исправлении для Red Hat-платформ, которая привела к тому, что vsftpd dthcbb 2.0.5 не освобождает распределенную память при обработке пользовательских команд, если включена опция deny_file в конфигурационном файле vsftpd.conf. Удаленный пользователь может подключиться к удаленному серверу, выполнить большое количество CWD-команд и потребить все доступные ресурсы на системе.

URL производителя: www.redhat.com.

Решение: Установите исправление с сайта производителя.

Множественные уязвимости в MDAemon

Программа: MDAemon 9.6.5, возможно, более ранние версии.

Опасность: Средняя.

Описание: 1. Уязвимость существует из-за ошибки разменовывания нулевого указателя при обработке HTTP-запросов, отправленных интерфейсу WordClient (порт 3000/TCP). Удаленный пользователь может с помощью специально сформированного HTTP POST-запроса, отправленного WorldClient.dll, аварийно завершить работу службы WordClient.

2. Уязвимость существует из-за ошибки проверки границ данных в WordClient-интерфейсе при обработке Reply-запросов с, например, слишком длинным полем Subject. Удаленный пользователь может с помощью специально сформированного e-mail-сообщения вызвать переполнение стека и выполнить произвольный код на целевой системе. Для успешной эксплуатации уязвимости требуется действительная учетная запись.

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

Решение: В настоящее время способов устранения уязвимости не существует.

Составил Александр Антипов