

Множественные уязвимости в Microsoft SQL Server

Программа: Microsoft Windows 2000 Server; Microsoft Windows 2003; Microsoft Windows 2008; Microsoft Data Engine (MSDE) 1.0; Microsoft SQL Server 7; Microsoft SQL Server 2000; Microsoft SQL Server 2000 Desktop Engine; Microsoft SQL Server 2005.

Опасность: Низкая.

Описание: 1. Уязвимость существует из-за ошибки в механизме повторного использования страниц памяти. Пользователи с привилегиями доступа оператора к базе данных могут получить доступ к потенциально важным данным (например, к данным сессии другого пользователя).

2. Уязвимость существует из-за ошибки проверки границ данных в функции конвертации при конвертации SQL-выражений из одного типа данных в другой. Удаленный пользователь может с помощью слишком длинного SQL-запроса повысить свои привилегии на системе.

3. Уязвимость существует из-за ошибки при обработке файлов резервных копий. Удаленный пользователь может с помощью RESTORE TSQL-запроса вызвать переполнение динамической памяти и выполнить произвольный код на целевой системе.

4. Уязвимость существует из-за ошибки проверки границ данных при обработке INSERT-запросов. Злоумышленник может с помощью специально сформированного INSERT-запроса вызвать переполнение буфера и повысить свои привилегии на системе.

URL производителя: www.microsoft.com.

Решение: Установите исправление с сайта производителя.

Отказ в обслуживании в Ruby

Программа: Ruby 1.8.x.

Опасность: Низкая.

Описание: Целочисленное переполнение обнаружено в функции `rb_ary_fill()` при обработке слишком длинного списка аргументов. Удаленный пользователь может вызвать переполнение динамической памяти и аварийно завершить работу уязвимого приложения.

URL производителя: www.ruby-lang.org/en.

Решение: Установите исправление из SVN-репозитория производителя.

Отказ в обслуживании в OpenLDAP

Программа: OpenLDAP 2.3.41, возможно, более ранние версии.

Опасность: Низкая.

Описание: Уязвимость существует из-за ошибки в функции `ber_get_next()` в файле `libraries/liblber/io.c`. Удаленный пользователь может с помощью специально сформированного ASN.1 BER-пакета выполнить вызов `assert()` и завершить процесс `slapd`.

URL производителя: www.openldap.org.

Решение: Установите исправление из CVS-репозитория производителя.

Повышение привилегий в Perl

Программа: Perl 5.10.

Опасность: Низкая.

Описание: Уязвимость существует из-за небезопасного использования команды `chmod` для символических ссылок в `File::Path::rmtree`. Локальный пользователь может с помощью специально сформированной символической ссылки установить привилегии на доступ 0777 для произвольных файлов на системе.

URL производителя: www.perl.org.

Решение: В настоящее время способов устранения уязвимости не существует.

Отказ в обслуживании в Sun Solaris

Программа: Sun Solaris 8, 9, 10.

Опасность: Низкая.

Описание: Уязвимость существует из-за неизвестной ошибки в Solstice Enterprise SNMP-DMI mapper subagent daemon (`snmpXdmid`). Удаленный пользователь может с помощью специально сформированного пакета вызвать отказ в обслуживании службы.

URL производителя: www.sun.com.

Решение: Установите исправление с сайта производителя.

Уязвимость при обработке IMAP-команд в SurgeMail

Программа: SurgeMail версии до 3.9g2.

Опасность: Низкая.

Описание: Уязвимость существует из-за неизвестной ошибки при обработке IMAP-команд. Удаленный пользователь может с помощью специально сформированной IMAP-команды аварийно завершить работу приложения.

URL производителя: www.netwinsite.com/surgemail.

Решение: Установите последнюю версию 3.9g2 с сайта производителя.

Переполнение буфера в PCRE

Программа: PCRE 7.7, возможно, более ранние версии.

Опасность: Средняя.

Описание: Уязвимость существует из-за ошибки в `pcre_compile.c` при обработке определенных шаблонов, содержащих вначале опцию и множественные разветвления. Удаленный пользователь может с помощью специально сформированных шаблонов вызвать переполнение динамической памяти и выполнить произвольный код на целевой системе.

URL производителя: www.pcre.org.

Решение: В настоящее время способов устранения уязвимости не существует.

Составил Александр Антипов