

Спуфинг-атака в OpenBSD

Программа: OpenBSD 4.2 и более ранние версии.

Опасность: Средняя.

Описание: Уязвимость существует из-за ошибки в генераторе псевдослучайных чисел (PRNG) в OpenBSD DNS-сервере. Злоумышленник может заполучить идентификатор DNS-транзакции и отравить кэш DNS-сервера.

URL производителя: www.openbsd.org.

Решение: В настоящее время способов устранения уязвимости не существует.

Множественные уязвимости в Adobe Flash Media Server

Программа: Adobe Flash Media Server 2.0.4 и более ранние версии; Adobe Connect Enterprise Server 6.

Опасность: Высокая.

Описание: 1. Целочисленное переполнение обнаружено в компоненте Edge Server при обработке RTMP (Real Time Message Protocol)-сообщений. Удаленный пользователь может отправить специально сформированный пакет на порт приложения 1935/TCP или 19350/TCP, вызвать переполнение динамической памяти и выполнить произвольный код на целевой системе.

2. Уязвимость существует из-за ошибки в компоненте Edge Server при обработке RTMP-запросов. Удаленный пользователь может с помощью специально сформированной последовательности запросов вызвать повреждение памяти и выполнить произвольный код на целевой системе.

URL производителя: www.adobe.com.

Решение: Установите последнюю версию Adobe Flash Media Server 2.0.5 или Adobe Connect 6 Service Pack 3 Update с сайта производителя.

Переполнение буфера в Symantec Veritas Storage Foundation

Программа: Symantec Veritas Storage Foundation 5.0.

Опасность: Средняя.

Описание: Уязвимость существует из-за ошибки проверки входных данных в Administrator Service. Удаленный пользователь может отправить специально сформированный пакет на порт 3207/UDP, вызвать переполнение динамической памяти и выполнить произвольный код на целевой системе.

URL производителя: www.symantec.com.

Решение: Установите исправление с сайта производителя.

Переполнение буфера в Mozilla Thunderbird

Программа: Mozilla Thunderbird 2.0.0.9, возможно более ранние версии.

Опасность: Высокая.

Описание: Уязвимость существует из-за ошибки при обработке external-body MIME-типов данных. Удаленный пользователь может с помощью специально сформированного e-mail-сообщения вызвать переполнение динамической памяти и выполнить произвольный код на целевой системе.

URL производителя: www.mozilla.com/en-US/thunderbird.

Решение: Установите последнюю версию 2.0.0.12 с сайта производителя.

Скриптинг между зонами в Skype

Программа: Skype для Windows 3.6.*.244 и более ранние версии.

Опасность: Высокая.

Описание: Skype использует Internet Explorer для воспроизведения HTML-форм на определенных веб-сайтах (DailyMotion, Metacafe и SkypeFind). Поскольку код выполняется в контексте безопасности «Local Machine», злоумышленник может выполнить произвольный код сценария на целевой системе посредством XSS-уязвимости на вышеперечисленных сайтах.

Вышеописанные сайты содержат уязвимости, которые позволяют злоумышленнику скомпрометировать целевую систему, когда пользователь просматривает видеогалерею с помощью Skype.

URL производителя: www.skype.com/products/skype/windows.

Решение: Установите последнюю версию 3.6.*.248 или выше с сайта производителя.

Загрузка произвольных файлов в Symantec Backup Exec System Recovery

Программа: Symantec Backup Exec System Recovery версии 7.0 и 7.0.1

Опасность: Средняя.

Описание: Уязвимость существует из-за ошибки в классе FileUpload, запущенном на Symantec LiveState Apache Tomcat-сервере. Удаленный пользователь может с помощью специально сформированного HTTP POST-запроса загрузить произвольные файлы на сервер.

URL производителя: www.symantec.com.

Решение: Установите последнюю версию 7.0.3 с сайта производителя.

Несколько уязвимостей в IBM DB2

Программа: IBM DB2 Universal Database версии до 8.2 Fixpak 16.

Опасность: Средняя.

Описание: 1. Уязвимость существует из-за неизвестной ошибки в утилите DB2PD. Локальный пользователь может получить root-привилегии на системе.

2. Уязвимость существует из-за ошибки проверки границ данных в DAS-сервере. Удаленный пользователь может вызвать переполнение буфера и вызвать отказ в обслуживании приложения.

3. Уязвимость существует из-за ошибки в механизме SYSPROC.ADMIN_SP_C. Подробности уязвимости не сообщаются.

4. Уязвимость существует из-за ошибки при обработке ALTER TABLE-запросов. Злоумышленник может обойти некоторые ограничения безопасности.

URL производителя: www-3.ibm.com/software/data/db2.

Решение: Способов устранения уязвимости не существует в настоящее время. Уязвимости будут исправлены в версии 8.2 Fixpak 16.

Составил Александр Антипов