

## Множественные уязвимости в IBM DB2

**Программа:** IBM DB2 для Linux UNIX и Windows 9.x.

**Опасность:** Средняя.

**Описание:** 1. Уязвимость существует из-за ошибки при обработке CONNECT/ATTACH. Удаленный пользователь может произвести DoS-атаку.

2. Уязвимость существует из-за ошибок в SYSPROC.ADMIN\_SP\_C, SYSPROC.NNSTAT и JARFILE ADMINISTRATION ROUTINES. Подробности уязвимости не сообщаются.

**URL производителя:** [www.ibm.com](http://www.ibm.com).

**Решение:** Установите исправление Fixpak 4a с сайта производителя.

## Обход ограничений безопасности в NetBSD

**Программа:** NetBSD 3.1.

**Опасность:** Средняя.

**Описание:** Уязвимость существует из-за того, что функция `ipsec4_get_ulp()` предполагает, что поле «`ip_off`» IPsec-пакета соответствует формату хоста. Злоумышленник может обойти IPsec-политики, если хотя бы две системы с различным порядком байт, подключены к целевой системе. Для успешной эксплуатации уязвимости ядро должно быть собрано с опцией FAST\_IPSEC.

**URL производителя:** [www.netbsd.org](http://www.netbsd.org).

**Решение:** Установите исправление с сайта производителя.

## Отказ в обслуживании в OpenBSD

**Программа:** OpenBSD 4.1 и 4.2, возможно более ранние версии.

**Опасность:** Средняя.

**Описание:** 1. Уязвимость существует из-за ошибки в функции `ip6_check_rh0hdr()` в файле `sys/netinet6/ip6_input.c`. Удаленный пользователь может с помощью IPV6-пакета, содержащего специально сформированные маршрутизационные заголовки, вызвать панику ядра системы. Уязвимость существует в OpenBSD 4.2.

2. Уязвимость существует из-за ошибки в функции `tcp_respond()` в файле `sys/netinet/tcp_subr.c`. Удаленный пользователь может с помощью специально сформированного TCP-пакета вызвать панику ядра системы.

**URL производителя:** [www.openbsd.org](http://www.openbsd.org).

**Решение:** Установите исправление с сайта производителя.

## Переполнение буфера в D-Link MPEG4 SHM Control ActiveX-компоненте

**Программа:** D-Link MPEG4 SHM (Audio) Control 1.7.0.5, возможно более ранние версии.

**Опасность:** Высокая.

**Описание:** Уязвимость существует из-за ошибки проверки границ данных в `VAPgDecoder.VaPgCtrl.1` ActiveX-компоненте (`VAPGDecoder.dll`) при обработке значений, передаваемых свойству «`Url`». Удаленный пользователь может с помощью специально сформированного веб-сайта вызвать переполнение стека и выполнить произвольный код на целевой системе.

**URL производителя:** [www.dlink.com](http://www.dlink.com).

**Решение:** В настоящее время способов устранения уязвимости не существует.

## Выполнение произвольного кода в Microsoft WebDAV Mini-Redirector

**Программа:** Microsoft Windows Server 2003 Datacenter Edition, Microsoft Windows Server 2003 Enterprise Edition, Microsoft Windows Server 2003 Standard Edition, Microsoft Windows Server 2003 Web Edition, Microsoft Windows Storage Server 2003, Microsoft Windows Vista, Microsoft Windows XP Home Edition, Microsoft Windows XP Professional.

**Опасность:** Высокая.

**Описание:** Уязвимость существует из-за ошибки в WebDAV Mini-Redirector (служба Web Client) при обработке длинных путей в WebDAV-ответах. Удаленный пользователь может с помощью специально сформированного WebDAV-ответа вызвать повреждение динамической памяти и выполнить произвольный код на целевой системе.

**URL производителя:** [www.microsoft.com](http://www.microsoft.com).

**Решение:** Установите исправление с сайта производителя.

## Переполнение буфера в VLC Media Player

**Программа:** VLC Media Player 0.8.6d, возможно более ранние версии.

**Опасность:** Высокая.

**Описание:** Уязвимость существует из-за ошибки проверки границ данных в MP4 demuxer (`modules/demux/mp4/mp4.c`). Удаленный пользователь может с помощью специально сформированного MPEG-4-файла перезаписать произвольные участки памяти и выполнить произвольный код на целевой системе.

**URL производителя:** [www.videolan.org/vlc](http://www.videolan.org/vlc).

**Решение:** Установите исправление с сайта производителя.

## Переполнение буфера в Novell Client

**Программа:** Novell Client для Windows NT/2000/XP 4.91 SP2, SP3 и SP4.

**Опасность:** Средняя.

**Описание:** Уязвимость существует из-за ошибки в `NWSPool.DLL` при обработке функции `EnumPrinters()`. Удаленный пользователь может с помощью специально сформированного RPC-запроса вызвать переполнение стека и выполнить произвольный код на целевой системе.

**URL производителя:** [www.novell.com/products/clients/windows/xp2000/overview.html](http://www.novell.com/products/clients/windows/xp2000/overview.html).

**Решение:** Установите исправление с сайта производителя (491psp2\_3\_4\_nwspool\_2.zip).

## Отказ в обслуживании в KAME Project

**Программа:** KAME Project.

**Опасность:** Средняя.

**Описание:** Уязвимость существует из-за ошибки в функции `ipcomp6_input()` в файле `kame/sys/netinet6/ipcomp_input.c` при обработке IPv6-пакетов, содержащих заголовки `IPComp`. Удаленный пользователь может с помощью специально сформированного IPv6-пакета вызвать отказ в обслуживании системы.

**URL производителя:** [www.kame.net](http://www.kame.net).

**Решение:** Установите исправление из CVS-репозитория производителя.

Составил Александр Антипов