

## Множественные уязвимости в IBM DB2

**Программа:** IBM DB2 8 версии до Fixpak 17.

**Опасность:** Средняя.

**Описание:** 1. Уязвимость существует из-за неизвестной ошибки при обработке CONNECT и ATTACH-запросов. Удаленный пользователь может вызвать отказ в обслуживании приложения.

2. Уязвимость существует из-за неизвестной ошибки, относящейся к DB2FMP-процессам. Подробности уязвимости не разглашаются.

**URL производителя:** [www-3.ibm.com/software/data/db2](http://www-3.ibm.com/software/data/db2).

**Решение:** Установите исправление Fixpak 17 с сайта производителя.

## Отказ в обслуживании в NetBSD

**Программа:** NetBSD 4.0.

**Опасность:** Средняя.

**Описание:** Уязвимость существует из-за ошибки деления на ноль при обработке ICMPv6-сообщений. Удаленный пользователь может с помощью специально сформированного ICMPv6 MLD-QUERY-пакета, в котором поле Maximum-Response-Delay установлено в значение, меньше чем 0x0010, вызвать отказ в обслуживании системы.

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

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

## Отказ в обслуживании в FreeBSD

**Программа:** FreeBSD 6.x, 7.0.

**Опасность:** Средняя.

**Описание:** Уязвимость существует из-за ошибки в функции icmp6\_mtudisc\_update() в файле src/sys/netinet6/icmp6.c при обработке ICMPv6-сообщений «Packet Too Big». Удаленный пользователь может с помощью специально сформированного ICMPv6-сообщения вызвать панику IPv6-стека.

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

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

## Уязвимости при обработке СНМ-файлов в ClamAV

**Программа:** ClamAV версии до 0.94.

**Опасность:** Средняя.

**Описание:** 1. Уязвимость существует из-за ошибки в файле libclamav/chmunpack.c при обработке СНМ. Удаленный пользователь может с помощью специально сформированного СНМ-файла заставить приложение обратиться к некорректному адресу в памяти и аварийно завершить свою работу.

2. Уязвимость существует из-за ошибки разыменования нулевого указателя в libclamav. Удаленный пользователь может вызвать отказ в обслуживании приложения.

3. Уязвимости существуют из-за утечки памяти в freshclam/manager.c. Удаленный пользователь может потратить все доступные ресурсы на системе.

4. Уязвимость существует из-за неизвестных ошибок, относящихся к error path, в libclamav/others.c и libclamav/sis.c.

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

**Решение:** Установите последнюю версию 0.94 с сайта производителя.

## Множественные уязвимости в Cisco ASA и PIX

**Программа:** Cisco PIX 7.x; Cisco PIX 8.x; Cisco Adaptive Security Appliance (ASA) 7.x, 8.x.

**Опасность:** Средняя.

**Описание:** 1. Уязвимость существует из-за неизвестной ошибки при обработке SIP-пакетов. Удаленный пользователь может перезагрузить устройство с включенной проверкой SIP. Уязвимости подвержены Cisco PIX и ASA версии до 7.0(7)16, 7.1(2)71, 7.2(4)7, 8.0(3)20 и 8.1(1)8.

2. Уязвимость существует из-за неизвестной ошибки, когда устройства Cisco PIX и Cisco ASA настроены на завершение клиентских VPN-подключений. Удаленный пользователь может перезагрузить устройство. Для успешной эксплуатации уязвимости злоумышленник должен иметь действительные учетные данные. Уязвимости подвержены Cisco PIX и Cisco ASA версии до 7.2(4)2, 8.0(3)14 и 8.1(1)4. Версии 7.0 и 7.1 не уязвимы.

3. Уязвимость существует из-за утечки памяти в Cisco ASA-устройствах, сконфигурированных на завершение безклиентных VPN-соединений. Удаленный пользователь может с помощью специально сформированного SSL или HTTP-пакета вызвать перезагрузку устройства. Уязвимости подвержены Cisco ASA версии до 7.2(4)2, 8.0(3)14 и 8.1(1)4. Версии 7.0 и 7.1 не уязвимы.

4. Уязвимость существует из-за ошибки при обработке URI в Cisco ASA-устройствах, которые завершают безклиентные удаленные VPN-соединения. Удаленный пользователь может вызвать перезагрузку устройства. Уязвимости подвержены Cisco ASA версии до 8.0(3)15, and 8.1(1)5. Версии 7.0, 7.1 и 7.2 не уязвимы.

5. Уязвимость существует из-за неизвестной ошибки в Cisco ASA-устройствах, сконфигурированных на завершение безклиентных VPN-соединений. Злоумышленник может обманом заставить пользователя посетить специально сформированный веб-сайт или ответить на e-mail и получить доступ к именам пользователей и паролям. Уязвимости подвержены Cisco ASA-устройства версии до 8.0 или 8.1 с включенной поддержкой безклиентных VPN. Версии 7.0, 7.1 и 7.2 не уязвимы.

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

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

## Множественные уязвимости в VMware ESX Server

**Программа:** VMware ESX Server 2.x.

**Опасность:** Средняя.

**Описание:** 1. Уязвимость существует из-за ошибки в библиотеке libpng. Удаленный пользователь может вызвать отказ в обслуживании.

2. Уязвимость существует из-за использования уязвимого кода библиотеки freetype. Удаленный пользователь может скомпрометировать целевую систему.

**URL производителя:** [www.vmware.com/products/server/esx\\_features.html](http://www.vmware.com/products/server/esx_features.html).

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

Составил Александр Антипов