

## Переполнение буфера в JustSystems Ichitaro

**Программа:** JustSystems Ichitaro 2005, 2006, 2007.

**Опасность:** Критическая.

**Описание:** Уязвимость существует из-за ошибки проверки границ данных в jsdci.dll при обработке .jtd-документов. Удаленный пользователь может с помощью специально сформированного .jtd-файла вызвать переполнение стека и выполнить произвольный код на целевой системе.

**Примечание:** Уязвимость активно эксплуатируется в настоящее время.

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

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

## Множественные уязвимости в ClamAV

**Программа:** Clam AntiVirus (ClamAV) версии до 0.92.

**Опасность:** Высокая.

**Описание:** 1. Целочисленное переполнение обнаружено в функции cli\_scanpe() при обработке MEW-запакованных исполняемых файлов. Удаленный пользователь может установить специально сформированные значения для «ssize» и «dsize», вызвать переполнение динамической памяти и выполнить произвольный код на целевой системе.

2. Уязвимость существует из-за ошибки завышения на единицу в файле libclamav/mspack.c при обработке MSZIP-архивов. Удаленный пользователь может с помощью специально сформированного MSZIP-архива выполнить произвольный код на целевой системе.

3. Уязвимость существует из-за ошибки проверки границ данных в bzrip2-макросах декомпрессии BZ\_GET\_FAST() и BZ\_GET\_FAST\_C() в файле libclamav/nsis/bzlib\_private.h.

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

**Решение:** Установите последнюю версию 0.92 с сайта производителя.

## Множественные уязвимости в Opera

**Программа:** Opera версии до 9.25.

**Опасность:** Высокая.

**Описание:** 1. Уязвимость существует из-за неизвестной ошибки в некоторых плагинах, которая позволяет удаленному пользователю произвести атаку типа «междоменный скриптинг» и выполнить произвольный код сценария в браузере жертвы.

2. Уязвимость существует из-за неизвестной ошибки при обработке TLS-сертификатов. Удаленный пользователь может выполнить произвольный код на целевой системе.

3. Уязвимость существует из-за неизвестной ошибки в Rich text-редакторе во время использования designMode. Удаленный пользователь может произвести атаку типа междоменный скриптинг и выполнить произвольный код сценария в браузере жертвы.

4. Уязвимость существует из-за ошибки при обработке bitmap-карт. Удаленный пользователь может получить доступ к содержимому произвольных ячеек памяти.

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

**Решение:** Установите последнюю версию 9.25 с сайта производителя.

## Повреждение памяти в FreeBSD

**Программа:** FreeBSD 6.2.

**Опасность:** Средняя.

**Описание:** Уязвимость существует из-за ошибки завышения на единицу в функции inet\_network(). Злоумышленник может передать специально сформированный аргумент уязвимой функции и вызвать переполнение буфера. Удачная эксплуатация уязвимости позволит злоумышленнику вызвать отказ в обслуживании приложения, использующего функцию inet\_network() без предварительной проверки входных данных, или выполнить произвольный код на целевой системе.

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

**Решение:** Установите исправление от производителя.

## Повышение привилегий в службе LSASS в Microsoft Windows

**Программа:** Microsoft Windows 2000, Microsoft Windows XP, Microsoft Windows 2003.

**Опасность:** Низкая.

**Описание:** Уязвимость существует из-за ошибки в службе Local Security Authority Subsystem Service (LSASS). Злоумышленник может с помощью специально сформированного LPC-запроса выполнить произвольный код на системе с привилегиями учетной записи SYSTEM.

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

**Решение:** Установите исправление от производителя.

## Повышение привилегий в Novell ZENworks Endpoint Security Management

**Программа:** Novell ZENworks Endpoint Security Management 3.5, возможно, более ранние версии.

**Опасность:** Низкая.

**Описание:** Уязвимость существует из-за того, что во время генерации отчета диагностики служба STEngine пытается выполнить командную оболочку, находящуюся в определенной директории с небезопасными привилегиями на доступ. Злоумышленник может поместить «cmd.exe» в директорию и выполнить произвольные команды на системе с привилегиями SYSTEM.

**URL производителя:** [www.novell.com/products/zenworks/endpointsecuritymanagement](http://www.novell.com/products/zenworks/endpointsecuritymanagement).

**Решение:** Установите последнюю версию 3.5.0.82 с сайта производителя.

## Ошибка завышения на единицу в ISC BIND

**Программа:** BIND 8 (все версии), BIND 9.0 (все версии), BIND 9.1 (все версии), BIND 9.2 (все версии), BIND 9.3.0, 9.3.1, 9.3.2, 9.3.3 и 9.3.4, BIND 9.4.0, 9.4.1 и 9.4.2, BIND 9.5.0a1, 9.5.0a2, 9.5.0a3, 9.5.0a4, 9.5.0a5, 9.5.0a6, 9.5.0a7 и 9.5.0b1.

**Опасность:** Низкая.

**Описание:** Уязвимость существует в приложениях, использующих библиотеку libbind.

**URL производителя:** [www.isc.org/index.pl?sw/bind/index.php](http://www.isc.org/index.pl?sw/bind/index.php).

**Решение:** Установите последнюю версию 9.3.5, 9.4.3, 9.5.0b2 или выше с сайта производителя.

Составил Александр Антипов