

Выполнение произвольного кода в Microsoft Works Image Server ActiveX-компоненте

Программа: Microsoft Works 7.x.

Опасность: Критическая.

Описание: Уязвимость существует из-за ошибки в Microsoft Works Image Server ActiveX-компоненте в библиотеке WkimgSrv.dll (clsid:00E1DB59-6EFD-4CE7-8C0A-2DA3BCAAD9C6). Удаленный пользователь может с помощью специально сформированного веб-сайта выполнить произвольный код на целевой системе.

URL производителя: www.microsoft.com.

Решение: В настоящее время способов устранения уязвимости не существует. В качестве временного решения рекомендуется аннулировать элемент управления ActiveX.

Множественные уязвимости в Opera

Программа: Opera версии до 9.27.

Опасность: Высокая.

Описание: 1. Уязвимость существует из-за ошибки в функционале, запрашивающем у пользователя разрешение на добавление нового новостного канала. Удаленный пользователь может с помощью специально сформированного новостного канала вызвать повреждение памяти и выполнить произвольный код на целевой системе.

2. Уязвимость существует из-за ошибки при обработке HTML CANVAS-элементов. Удаленный пользователь может с помощью специально сформированных изображений вызвать повреждение памяти и выполнить произвольный код на целевой системе.

URL производителя: www.opera.com.

Решение: Установите последнюю версию 9.27 с сайта производителя.

Несколько уязвимостей в IBM DB2

Программа: DB2 Universal Database 8.x; IBM DB2 for Linux UNIX and Windows 9.x.

Опасность: Низкая.

Описание: 1. Уязвимость существует из-за ошибки проверки границ данных в setuid-приложении db2dasrrm. Локальный пользователь может с помощью слишком длинного значения переменной окружения DASPROF вызвать переполнение стека и выполнить произвольный код на целевой системе с привилегиями учетной записи root.

2. Уязвимость существует из-за того, что при запуске приложения db2dasrrm файлы dasRecoveryIndex, dasRecoveryIndex.tmp, .dasRecoveryIndex.lock и dasRecoveryIndex.cor создаются небезопасным образом. Локальный пользователь может с помощью специально сформированной символической ссылки перезаписать произвольные файлы на системе с привилегиями пользователя root. Для успешной эксплуатации уязвимости злоумышленник должен иметь привилегии на запуск DB2 Administration Server (быть членом групп dasusr1 или db2adm1).

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

Решение: Установите исправление с сайта производителя.

Множественные уязвимости в ClamAV

Программа: ClamAV 0.92 и 0.92.1, возможно, более ранние версии.

Опасность: Высокая.

Описание: 1. Уязвимость существует из-за ошибки проверки границ данных в функции cli_scanpe() в файле libclamav/re.c. Удаленный пользователь может с помощью специально сформированного выполняемого Upack-файла вызвать переполнение динамической памяти и выполнить произвольный код на целевой системе.

2. Уязвимость существует из-за ошибки проверки границ данных при обработке PeSpin-пакованных исполняемых файлов в libclamav/spin.c. Удаленный пользователь может вызвать переполнение динамической памяти и выполнить произвольный код на целевой системе.

3. Уязвимость существует из-за неизвестной ошибки при обработке ARJ-файлов. Удаленный пользователь может с помощью специально сформированного ARJ-файла вызвать зависание приложения.

4. Уязвимость существует из-за ошибки проверки границ данных в libclamav/re.c при обработке WWPack-пакованных PE-файлов. Удаленный пользователь может вызвать повреждение динамической памяти и выполнить произвольный код на целевой системе.

URL производителя: www.clamav.net.

Решение: Установите последнюю версию 0.93 с сайта производителя.

Обход ограничений безопасности в Sun Java System Directory Server

Программа: Sun Java System Directory Server 6.0, 6.1, 6.2, Enterprise Edition.

Опасность: Высокая.

Описание: Уязвимость существует из-за неизвестной ошибки при определении соединений, основанных на bind-dn. Удаленный пользователь может получить административный доступ к приложению.

URL производителя: www.sun.com/software/products/directory_srvr_ee.

Решение: Установите последнюю версию 6.3 с сайта производителя.

Повреждение памяти в Mozilla Firefox

Программа: Mozilla Firefox версии до 2.0.0.14.

Опасность: Низкая.

Описание: Уязвимость существует из-за неизвестной ошибки в механизме JavaScript в JavaScript Garbage Collector. Удаленный пользователь может с помощью специально сформированного веб-сайта вызвать повреждение памяти и аварийно завершить работу браузера. Возможность выполнения произвольного кода не подтверждена.

URL производителя: www.mozilla.org.

Решение: Установите последнюю версию 2.0.0.14 с сайта производителя.

Составил Александр Антипов