

Выполнение произвольного кода в Mozilla Firefox

Программа: Mozilla Firefox 2.0.x и 3.0.

Опасность: Высокая.

Описание: Уязвимость существует из-за неизвестной ошибки, которая может позволить удаленному пользователю выполнить произвольный код на целевой системе.

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

Решение: В настоящее время способов устранения уязвимости не существует.

Выполнение произвольного кода в Opera

Программа: Opera версии до 9.51.

Опасность: Высокая.

Описание: Уязвимость существует из-за неизвестной ошибки, которая позволяет удаленному пользователю выполнить произвольный код на целевой системе. Подробности уязвимости не раскрываются.

URL производителя: www.opera.com.

Решение: Установите последнюю версию 9.51 с сайта производителя.

Множественные уязвимости в Apple Safari для Windows

Программа: Apple Safari for Windows версии до 3.1.2; Apple Safari версии до 3.1.2.

Опасность: Высокая.

Описание: 1. Уязвимость существует из-за ошибки проверки границ данных при обработке BMP- и GIF-изображений. Удаленный пользователь может с помощью специально сформированного BMP- или GIF-изображения просмотреть произвольные участки памяти.

2. Уязвимость существует из-за того, что Safari автоматически запускает загрузку исполняемых файлов с сайтов, которые находятся в зоне Internet Explorer 7 с включенной опцией «Launching applications and unsafe files», или файлов с сайтов в зонах Local intranet или Trusted sites в браузере Internet Explorer 6.

3. Уязвимость существует из-за неизвестной ошибки при обработке Javascript-массивов. Удаленный пользователь может с помощью специально сформированного веб-сайта вызвать повреждение памяти и выполнить произвольный код на целевой системе.

URL производителя: www.apple.com/safari/download.

Решение: Установите последнюю версию 3.1.2 с сайта производителя.

Отравление DNS-кэша в ISC BIND

Программа: ISC BIND версии до 9.5.0-P1, 9.4.2-P1 и 9.3.5-P1.

Опасность: Средняя.

Описание: Уязвимость существует из-за того, что DNS-сервер использует предсказуемый номер порта для отправки DNS-запросов. Удаленный пользователь может произвести отравление DNS-кэша.

URL производителя: www.isc.org/products/BIND.

Решение: Установите последнюю версию 9.5.0-P1, 9.4.2-P1 или 9.3.5-P1 с сайта производителя.

Множественные уязвимости в Mozilla Firefox

Программа: Mozilla Firefox версии до 2.0.0.15.

Опасность: Высокая.

Описание: 1. Уязвимость существует из-за различных неизвестных ошибок. Удаленный пользователь может вызвать повреждение памяти и аварийно завершить работу приложения и выполнить произвольный код на целевой системе. Подробности уязвимости не раскрываются.

2. Уязвимость существует из-за неизвестной ошибки при загрузке кода сценария в контексте Chrome из fastload-файла. Удаленный пользователь может выполнить произвольный код на целевой системе.

3. Уязвимость существует из-за неизвестной ошибки в функции `mozIJSSubScriptLoader.loadSubScript()`. Удаленный пользователь может выполнить произвольный код.

4. Уязвимость существует из-за недостаточной обработки «File location» URL, полученных из списка директорий. Удаленный пользователь может скомпрометировать целевую систему.

5. Уязвимость существует из-за ошибки в block reflow-процессе. Удаленный пользователь может вызвать отказ в обслуживании браузера или выполнить произвольный код на целевой системе.

6. Уязвимость существует из-за ошибки, которая позволяет злоумышленнику обойти JavaScript same origin-политику и произвести XSS-нападение.

7. Уязвимость существует из-за неизвестной ошибки, которая относится к signed JAR tampering. Подробности уязвимости не раскрываются.

8. Уязвимость существует из-за неизвестной ошибки, которая позволяет удаленному пользователю с помощью элементов DOM Range и originalTarget загрузить произвольные файлы на систему.

9. Уязвимость существует из-за ошибки в реализации Java LiveConnect на системе Mac OS X. Удаленный пользователь может установить произвольные сетевые подключения.

10. Уязвимость существует из-за ошибки доступа к неинициализированной памяти при загрузке специально сформированного файла .properties.

11. Уязвимость существует из-за ошибки при обработке Alt Names в сертификатах. Удаленный пользователь может произвести спуфинг-атаку.

12. Уязвимость существует из-за ошибки при обработке ярлыков Windows, которая позволяет открыть внешний сайт как локальный файл.

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

Решение: Установите последнюю версию 2.0.0.15 с сайта производителя.

Составил Александр Антипов