

Множественные уязвимости в Sun Java JDK / JRE

Программа: Sun Java JDK 1.5.x, Sun Java JDK 1.6.x, Sun Java JRE 1.4.x, Sun Java JRE 1.5.x / 5.x, Sun Java JRE 1.6.x/6.x, Sun Java SDK 1.4.x, Java Web Start 1.x, Java Web Start 6.x.

Опасность: Высокая.

Описание: 1. Две уязвимости обнаружены в Java Runtime Environment Virtual Machine. Удаленный пользователь может с помощью недоверенного апплета просмотреть содержимое произвольных файлов, записать файлы на систему и выполнить локальные приложения.

2. Уязвимость существует из-за неизвестной ошибки в Java Runtime Environment (JRE) при обработке XSLT-трансформаций. Удаленный пользователь может с помощью специально сформированного недоверенного апплета или приложения просмотреть произвольные URL-ресурсы или выполнить произвольный код на целевой системе.

3. Обнаружено три ошибки проверки границ данных в Java Web Start. Злоумышленник может с помощью недоверенного Java Web Start-приложения прочитать и записать локальные файлы и выполнить локальные приложения.

4. Уязвимость существует из-за неизвестной ошибки в Java Web Start. Удаленный пользователь может с помощью специально сформированного недоверенного апплета прочитать и записать локальные файлы и выполнить локальные приложения на системе.

5. Уязвимость существует из-за неизвестной ошибки в Java Web Start. Удаленный пользователь может с помощью специально сформированного Java Web Start-приложения создать произвольные файлы на системе и выполнить локальные приложения с привилегиями пользователя, запустившего недоверенное Java Web Start-приложение.

6. Уязвимость существует из-за неизвестной ошибки в Java-плагине. Удаленный пользователь может с помощью специально сформированного недоверенного апплета обойти ограничения политики «same origin» и выполнить локальные приложения на системе.

7. Уязвимость существует из-за ошибки в библиотеке обработки графических изображений в Java Runtime Environment при обработке ICC-профилей. Удаленный пользователь может аварийно завершить работу JVM, записать произвольные данные в файлы или выполнить локальные приложения.

8. Уязвимость существует из-за ошибки в Java Runtime Environment, которая позволяет Javascript-коду в браузере создать подключения Java API к сетевым службам на локальной системе.

9. Уязвимость существует из-за ошибки проверки границ данных в Java Web Start при обработке JNLP-файлов. Удаленный пользователь может с помощью специально сформированного веб-сайта вызвать переполнение стека и выполнить произвольный код на целевой системе.

URL производителя: www.sun.com.

Решение: Установите исправление с сайта производителя.

Повреждение памяти в Microsoft Office

Программа: Microsoft Office 2000 Service Pack 3, Microsoft Office XP Service Pack 3, Microsoft Office 2003 Service Pack 2, Microsoft Office Excel Viewer 2003 and Microsoft Office Excel Viewer Service Pack 3, Microsoft Office 2004 for Mac.

Опасность: Высокая.

Описание: 1. Уязвимость существует из-за ошибки при обработке BIFF File Format-записей в Excel-файлах. Удаленный пользователь может с помощью специально сформированного комментария к ячейке заставить приложение воссоздать поврежденные метаданные, используя указанное злоумышленником смещение, и выполнить произвольный код на целевой системе.

2. Уязвимость существует из-за ошибки при обработке документов. Удаленный пользователь может с помощью специально сформированного файла вызвать повреждение памяти и выполнить произвольный код на целевой системе.

URL производителя: www.microsoft.com.

Решение: Установите исправление с сайта производителя.

Выполнение произвольного кода в Microsoft Office Web Components

Программа: Microsoft Office Web Components 2000.

Опасность: Высокая.

Описание: 1. Уязвимость существует из-за ошибки при обработке URL в Microsoft Office Web Components. Удаленный пользователь может с помощью специально сформированной веб-страницы выполнить произвольный код на целевой системе.

2. Уязвимость существует из-за неизвестной ошибки в Microsoft Office Web Components. Удаленный пользователь может с помощью специально сформированного веб-сайта выполнить произвольный код на целевой системе.

URL производителя: www.microsoft.com.

Решение: Установите исправление с сайта производителя.

Уязвимость при обработке URI в Microsoft Outlook

Программа: Microsoft Outlook 2000 Service Pack 3, Microsoft Outlook 2002 Service Pack 3, Microsoft Outlook 2003 Service Pack 2, Microsoft Outlook 2003 Service Pack 3, Microsoft Outlook 2007.

Опасность: Высокая.

Описание: Уязвимость существует из-за ошибки при обработке URI в Microsoft Outlook. Удаленный пользователь может с помощью веб-сайта или e-mail-сообщения, содержащего специально сформированный «mailto:» URI, передать дополнительные параметры командной строки в Outlook и выполнить произвольный код на целевой системе. Для успешной эксплуатации уязвимости пользователь должен нажать на специально сформированную ссылку.

URL производителя: www.microsoft.com.

Решение: Установите исправление с сайта производителя.

Составил Александр Антипов