

Переполнение буфера в Novell eDirectory

Программа: Novell eDirectory 8.7.3 и 8.8, возможно, более ранние версии.

Опасность: Средняя.

Описание: Уязвимость существует из-за ошибки при подсчете размера буфера динамической памяти для сохранения параметров LDAP-поиска. Удаленный пользователь может с помощью специально сформированной строки вызвать переполнение динамической памяти и выполнить произвольный код на целевой системе.

URL производителя: www.novell.com/products/edirectory.

Решение: Установите исправление 8.8.2 FTF2 или 8.7.3.10b с сайта производителя.

Целочисленное переполнение в Pidgin

Программа: Pidgin версии до 2.4.3.

Опасность: Средняя.

Описание: Целочисленное переполнение обнаружено в функции `msn_slplink_process_msg` в файлах `libpurple/protocols/msnp9/slplink.c` и `libpurple/protocols/msn/slplink.c`. Удаленный пользователь может с помощью специально сформированного NSM SLP-сообщения выполнить произвольный код на целевой системе.

URL производителя: pidgin.im/pidgin/home.

Решение: Установите последнюю версию 2.4.3 с сайта производителя.

Обход ограничений безопасности в Red Hat Certificate System

Программа: Red Hat Certificate System 7.x.

Опасность: Средняя.

Описание: Уязвимость существует из-за ошибки при обработке расширений в запросах на подпись сертификатов (CSR), когда все требуемые расширения добавлены в выдаваемый сертификат. Удаленный пользователь может обойти некоторые политики безопасности, например, создать CSR-запрос для подчиненного CA-сертификата, что запрещено в конфигурации CA.

URL производителя: www.redhat.com/en_us/USA/home/solutions/rhcs.

Решение: Установите исправление с сайта производителя.

Отказ в обслуживании в ClamAV

Программа: ClamAV версии до 0.93.1.

Опасность: Средняя.

Описание: Уязвимость существует из-за ошибки проверки границ данных в `libclamav/petite.c`. Удаленный пользователь может с помощью специально сформированного Petite-пакета вызвать повреждение памяти и аварийно завершить работу приложения.

URL производителя: www.clamav.net.

Решение: Установите последнюю версию 0.93.1 с сайта производителя.

Множественные уязвимости в Sun Java JDK и JRE

Программа: Java Web Start 1.x; Java Web Start 5.x; Java Web Start 6.x; Sun Java JDK 1.5.x; Sun Java JDK 1.6.x; Sun Java JRE 1.3.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 1.3.x; Sun Java SDK 1.4.x.

Опасность: Высокая.

Описание: 1. Уязвимость существует из-за ошибки в Java Runtime Environment Virtual Machine, которая позволяет недоверенному апплету прочитать и записать локальные файлы и выполнить локальные приложения.

2. Уязвимость существует из-за ошибки в агенте управления Java Management Extensions (JMX), которая позволяет JMX-клиенту произвести определенные неавторизованные операции на системе с JMX с включенным локальным мониторингом.

3. Две ошибки обнаружены в механизме поддержки языковых сценариев в Java Runtime Environment. Недоверенные апплеты могут получить доступ к данным других апплетов, прочитать и записать локальные файлы и выполнить локальные приложения.

4. Уязвимость существует из-за ошибки проверки границ данных в Java Web Start. Злоумышленник может с помощью недоверенных Java Web Start-приложений вызвать переполнение буфера.

5. Три ошибки обнаружены в Java Web Start, которые позволяют недоверенным Java Web Start-приложениям определить местонахождение кеша Java Web Start и создать или удалить произвольные файлы на системе с привилегиями пользователя, запустившего Java Web Start-приложение.

6. Уязвимость существует из-за ошибки в реализации Secure Static Versioning, которая позволяет апплетам запускаться на старых версиях JRE.

7. Уязвимость существует из-за ошибок в Java Runtime Environment, которые позволяют недоверенному апплету обойти ограничения политики единства происхождения (same-origin policy) и создать сетевые подключения к различным службам на локальном хосте.

8. Уязвимость существует из-за ошибки в Java Runtime Environment при обработке некоторых XML-данных. Удаленный пользователь может получить неавторизованный доступ к определенным URL-ресурсам и вызвать отказ в обслуживании. Для успешной эксплуатации уязвимости требуется, чтобы JAX-WS-клиент или сервер были в списках доверенных приложений для обработки XML-данных.

9. Уязвимость существует из-за ошибки в Java Runtime Environment при обработке определенных XML-данных. Удаленный пользователь может с помощью недоверенного апплета или приложения получить неавторизованный доступ к определенным URL-ресурсам.

10. Уязвимость существует из-за ошибки проверки границ данных при обработке шрифтов в Java Runtime Environment. Удаленный пользователь может вызвать переполнение буфера.

URL производителя: java.sun.com.

Решение: Установите исправление с сайта производителя.

Составил Александр Антипов