

Уязвимость при обработке апплетов в Sun JRE

Программа: Sun Java JDK и JRE 6 Update 1 и более ранние версии; Sun Java JDK и JRE 5.0 Update 13 и более ранние версии.

Опасность: Высокая.

Описание: Уязвимость существует из-за неизвестной ошибки при обработке Java-апплетов. Удаленный пользователь может с помощью недоверенного апплета просмотреть содержимое или записать произвольные файлы на систему и выполнить произвольные приложения.

URL производителя: java.sun.com.

Решение: Установите последнюю версию или исправления с сайта производителя.

Множественные уязвимости в Mozilla Firefox

Программа: Mozilla Firefox версии до 2.0.0.12.

Опасность: Высокая.

Описание: 1. Обнаружены различные ошибки в движке браузера. Удаленный пользователь может с помощью специально сформированного веб-сайта вызвать повреждение памяти и выполнить произвольный код на целевой системе.

2. Уязвимость существует из-за различных ошибок в реализации JavaScript. Удаленный пользователь может с помощью специально сформированного веб-сайта вызвать повреждение памяти и выполнить произвольный код на целевой системе.

3. Уязвимость существует из-за ошибки дизайна при обработке фокуса. Злоумышленник может обманом заставить пользователя загрузить произвольные файлы на сервер.

4. Уязвимость существует из-за ошибки в реализации JavaScript. Злоумышленник может выполнить произвольный JavaScript-код с привилегиями «chrome».

5. Уязвимость существует из-за ошибки в реализации JavaScript. Удаленный пользователь может с помощью функции XMLHttpRequest.load() обойти ограничения same-origin-политики.

6. Уязвимость существует из-за ошибки при обработке графических изображений, когда пользователь покидает страницу, используя designMode-фреймы. Злоумышленник может получить доступ к истории посещения страниц пользователя, вызвать повреждение памяти и выполнить произвольный код на целевой системе.

7. Уязвимость существует из-за ошибки дизайна, связанной с использованием таймера в диалоговых окнах. Злоумышленник может обманом заставить пользователя нажать на кнопку в диалоговом окне безопасности.

8. Уязвимость существует из-за того, что браузер следует «302»-перенаправлению для загрузки файлов стилей и позволяет чтение целевого URL посредством element.sheet.href. Злоумышленник может получить доступ к потенциально важным параметрам URL.

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

Решение: Установите последнюю версию 2.0.0.12 с сайта производителя.

Множественные уязвимости в Cisco Unified IP Phone

Программа: Cisco Unified IP Phone 7900 Series.

Опасность: Высокая.

Описание: 1. Уязвимость существует из-за ошибки проверки границ данных при обработке DNS-ответов. Злоумышленник может с помощью специально сформированного DBS-ответа вызвать переполнение буфера и выполнить произвольный код на целевом устройстве.

2. Уязвимость существует из-за ошибки при обработке ICMP-пакетов. Удаленный пользователь может с помощью слишком большого ICMP echo-пакета вызвать перезагрузку устройства.

3. Уязвимость существует из-за ошибки при обработке HTTP-запросов. Удаленный пользователь может с помощью специально сформированного HTTP-запроса вызвать перезагрузку устройства.

4. Уязвимость существует из-за ошибки проверки границ данных в Secure Shell (SSH)-сервере. Удаленный пользователь может с помощью специально сформированного пакета вызвать переполнение буфера и перезагрузить устройство выполнить произвольный код.

5. Уязвимость существует из-за ошибки проверки границ данных при обработке кодированных данных Multipurpose Internet Mail Extensions (MIME). Удаленный пользователь может с помощью специально сформированного SIP-сообщения вызвать переполнение буфера и выполнить произвольный код на целевой системе.

6. Уязвимость существует из-за ошибки проверки границ данных в Telnet-сервере. Локальный непривилегированный пользователь может с помощью специально сформированной команды вызвать переполнение буфера и повысить свои привилегии на устройстве.

7. Уязвимость существует из-за ошибки проверки границ данных при обработке challenge/response-сообщений, полученных от SIP-прокси-сервера. Злоумышленник, контролирующий SIP-прокси, может отправить специально сформированное challenge/response-сообщений, вызвать переполнение динамической памяти и выполнить произвольный код на целевом устройстве.

URL производителя: www.cisco.com.

Решение: Установите последнюю версию прошивки с сайта производителя.

Множественные уязвимости в ClamAV

Программа: ClamAV версии до 0.92.1.

Опасность: Высокая.

Описание: 1. Целочисленное переполнение обнаружено в функции cli_scanpe() в файле libclamav/pe.c. Подробности уязвимости не сообщаются.

2. Уязвимость существует из-за ошибки в функции unmesh11() в файле libclamav/mew.c. Удаленный пользователь может вызвать повреждение памяти и выполнить произвольный код на целевой системе.

URL производителя: www.clamav.net.

Решение: Установите последнюю версию 0.92.1 с сайта производителя.

Составил Александр Антипов