

Уязвимость индексации массива в xine-lib

Программа: xine-lib 1.1.10.1, возможно, более ранние версии.

Опасность: Высокая.

Описание: Уязвимость существует из-за ошибки проверки границ данных в функции «sdpplin_parse()» в файле input/libreal/sdpplin.c. Удаленный пользователь может с помощью слишком длинного «streamid» SDP-параметра, включенного в RTSP-поток, выполнить произвольный код на целевой системе.

URL производителя: xinehq.de.

Решение: В настоящее время способов устранения уязвимости не существует.

Множественные уязвимости в Mozilla Firefox

Программа: Mozilla Firefox версии до 2.0.0.13.

Опасность: Высокая.

Описание: 1. Уязвимость существует из-за неизвестной ошибки в XPCNativeWrappers. Удаленный пользователь может с помощью функции setTimeout() выполнить произвольный Javascript-код с привилегиями пользователя.

2. Уязвимость существует из-за ошибки в механизме layout. Удаленный пользователь может вызвать повреждение памяти, и выполнить произвольный код на целевой системе.

3. Обнаружены различные уязвимости, которые позволяют злоумышленнику запустить Javascript-сценарии с повышенными привилегиями и выполнить произвольный код на целевой системе. Подробности уязвимостей не сообщаются.

4. Уязвимости существуют из-за неизвестной ошибки, которая позволяет злоумышленнику вызвать повреждение памяти и потенциально скомпрометировать целевую систему. Подробности уязвимостей не сообщаются.

5. Уязвимость существует из-за недостаточной обработки URL. Удаленный пользователь может с помощью специально сформированного URL подменить HTTP-заголовков «Referer».

6. Уязвимость существует из-за того, что браузер автоматически выбирает сертификат для SSL-аутентификации и позволяет злоумышленнику получить доступ к некоторым важным данным, указанным в сертификате (e-mail-адрес, имя пользователя и т. д.).

7. Уязвимость существует из-за ошибки при обработке данных, передаваемых по протоколу jar:. Удаленный пользователь может использовать Java посредством LiveConnect для открытия подключений к произвольным портам на локальной системе (localhost).

8. Уязвимость существует из-за того, что браузер позволяет создание XUL pop-up-окна на активной вкладке пользовательского браузера. Удаленный пользователь может подменить элементы форм, открытые на соседней вкладке, и похитить потенциально важные данные.

URL производителя: www.mozilla.com.

Решение: Установите последнюю версию 2.0.0.13 с сайта производителя.

Множественные уязвимости в Kerberos

Программа: Kerberos 5 1.6.3 и более ранние версии.

Опасность: Высокая.

Описание: 1. Уязвимость существует из-за того, что KDC использует глобальную переменную для всех входящих krb4-запросов, но устанавливает переменную только для некоторых запросов. Удаленный пользователь может получить доступ к важным данным, вызвать отказ в обслуживании или скомпрометировать целевую систему.

2. Уязвимость существует из-за ошибки в KDC при отправке ответов на krb4-запросы. Удаленный пользователь может получить доступ к потенциально важным данным.

3. Две уязвимости обнаружены в библиотеке Kerberos RPC при обработке дескрипторов открытых файлов. Удаленный пользователь может с помощью большого количества RPC-запросов вызвать повреждение памяти.

URL производителя: web.mit.edu/kerberos/www.

Решение: Установите исправление с сайта производителя.

Множественные уязвимости в WinRAR

Программа: WinRAR версии до 3.71.

Опасность: Высокая.

Описание: Уязвимости существуют из-за неизвестных ошибок при обработке архивов. Удаленный пользователь может с помощью специально сформированного архива вызвать повреждение динамической памяти или переполнение стека и выполнить произвольный код на целевой системе.

URL производителя: www.rarlabs.com.

Решение: Установите последнюю версию 3.71 с сайта производителя.

Множественные уязвимости в Asterisk

Программа: Asterisk 1.x, Asterisk Appliance Developer Kit 0.x, Asterisk Business Edition 2.x.

Опасность: Высокая.

Описание: 1. Уязвимость существует из-за ошибки в функции ast_rtp_unset_m_type() в файле main/rtp.c. Удаленный пользователь может с помощью специально сформированного SIP-пакета записать 0 в определенный участок памяти.

2. Уязвимость существует из-за ошибки проверки границ данных в функции process_sdp() в файле channels/chan_sip.c. Удаленный пользователь может отправить более 32 RTP-пейлоадов, вызвать переполнение стека и выполнить произвольный код на целевой системе.

3. Уязвимость существует из-за ошибки в SIP channel driver во время определения потребности в аутентификации. Удаленный пользователь может с помощью специально сформированного заголовка From произвести неавторизованные звонки.

4. Уязвимость существует из-за ошибки форматной строки в функции ast_verbose(). Удаленный пользователь может аварийно завершить работу приложения. Уязвимости подвержены версии до 1.6.0-beta6.

URL производителя: www.asterisk.org.

Решение: Установите последнюю версию с сайта производителя.

Составил Александр Антипов