

Переполнение буфера в Bea Weblogic Apache Connector

Программа: Bea Weblogic Server.

Опасность: Высокая.

Описание: Уязвимость существует из-за ошибки проверки границ данных в Apache-коннекторе. Удаленный пользователь может с помощью специально сформированного POST-запроса вызвать переполнение стека и выполнить произвольный код на целевой системе.

URL производителя: www.bea.com/framework.jsp?CNT=index.htm&FP=/content/products/weblogic/server.

Решение: В настоящее время способов устранения уязвимости не существует.

Переполнение буфера в Trend Micro OfficeScan

Программа: Trend Micro OfficeScan 7.3 build 1343(Patch 4), возможно, более ранние версии, Trend Micro OfficeScan Corporate Edition 8.x.

Опасность: Высокая.

Описание: Уязвимость существует из-за ошибки проверки границ данных в OfficeScan Corp Edition Web-Deployment ObjRemoveCtrl Class ActiveX-компоненте (OfficeScanRemoveCtrl.dll) в OfficeScan-клиенте при попытке отобразить список конфигурационных настроек. Удаленный пользователь может с помощью специально сформированного веб-сайта вызвать переполнение стека и выполнить произвольный код на целевой системе.

URL производителя: www.trendmicro.com/en/products/desktop/osce/evaluate/overview.htm.

Решение: Установите исправление с сайта производителя.

Множественные уязвимости в xine-lib

Программа: xine-lib версии до 1.1.15.

Опасность: Высокая.

Описание: 1. Множественные целочисленные переполнения обнаружены при обработке ID3-тегов в файле src/demuxers/id3.c. Удаленный пользователь может с помощью специально сформированного ID3-тега вызвать переполнение динамической памяти и выполнить произвольный код на целевой системе.

2. Уязвимость существует из-за ошибок проверки границ данных в функции demux_real_send_chunk() в файле src/demuxers/demux_real.c. Удаленный пользователь может с помощью специально сформированного Real Media-файла вызвать переполнение динамической памяти и выполнить произвольный код на целевой системе.

3. Уязвимость существует из-за ошибки проверки границ данных в функции open_video_capture_device() в файле src/input/input_v4l.c. Удаленный пользователь может с помощью специально сформированного V4L-потока вызвать переполнение динамической памяти и выполнить произвольный код на целевой системе.

URL производителя: xinehq.de.

Решение: Установите последнюю версию 1.1.15 с сайта производителя.

Переполнение буфера в Webex Meeting Manager WebexUCFObject ActiveX-компоненте

Программа: Webex Meeting Manager 20.2008.2601.4928, возможно, более ранние версии.

Опасность: Высокая.

Описание: Уязвимость существует из-за ошибки проверки границ данных в WebexUCFObject ActiveX-компоненте (atucfobj.dll) при обработке аргумента, передаваемого методу NewObject(). Удаленный пользователь может с помощью специально сформированного веб-сайта вызвать переполнение стека и выполнить произвольный код на целевой системе.

URL производителя: www.webex.com/downloads_webex.html.

Решение: Установите последнюю версию 20.2008.2606.4919 с сайта производителя.

Переполнение буфера в Microsoft Visual Studio

Программа: Microsoft Visual Studio 6.0, возможно, другие версии.

Опасность: Высокая.

Описание: Уязвимость существует из-за ошибки проверки границ данных в Masked Edit ActiveX-компоненте (Msmask32.ocx версии 6.0.81.69). Удаленный пользователь может с помощью специально сформированного веб-сайта передать уязвимому компоненту слишком длинный параметр Mask, вызвать переполнение стека и выполнить произвольный код на целевой системе.

URL производителя: msdn2.microsoft.com/en-us/library/ms950417.aspx.

Решение: Установите исправленную версию Msmask32.ocx 6.0.84.18 с сайта производителя.

Неавторизованное изменение пароля в Joomla

Программа: Joomla версии до 1.5.6.

Опасность: Средняя.

Описание: Уязвимость существует из-за некорректного ограничения доступа к сценарию components/com_user/models/reset.php. Удаленный пользователь может обойти механизм аутентификации и изменить пароль пользователя с наименьшим идентификатором в базе данных (как правило, администратора).

Пример: 1. Открыть страницу: [http://\[host\]/index.php?option=com_user&view=reset&layout=confirm](http://[host]/index.php?option=com_user&view=reset&layout=confirm).

2. Установить в поле «token» символ «”».

3. Указать новый пароль для учетной записи admin.

4. Перейти на страницу: [http://\[host\]/administrator](http://[host]/administrator).

5. Авторизоваться в приложении с новым паролем.

URL производителя: www.joomla.org.

Решение: Установите последнюю версию 1.5.6 с сайта производителя.

Составил Александр Антипов