

Множественные уязвимости в продуктах Oracle

Программа: Oracle Database 11g, версия 11.1.0.6; Oracle Database 10g Release 2, версии 10.2.0.2, 10.2.0.3; Oracle Database 10g, версия 10.1.0.5; Oracle Database 9i Release 2, версии 9.2.0.8, 9.2.0.8DV; Oracle Application Server 10g Release 3 (10.1.3), версии 10.1.3.1.0, 10.1.3.3.0; Oracle Application Server 10g Release 2 (10.1.2), версии 10.1.2.0.2, 10.1.2.1.0, 10.1.2.2.0; Oracle Application Server 10g (9.0.4), версия 9.0.4.3; Oracle Collaboration Suite 10g, версия 10.1.2; Oracle E-Business Suite Release 12, версия 12.0.4; Oracle E-Business Suite Release 11i, версия 11.5.10.2; Oracle PeopleSoft Enterprise PeopleTools версии 8.22.19, 8.48.16, 8.49.09; Oracle PeopleSoft Enterprise HCM версии 8.8 SP1, 8.9, 9.0.

Oracle Siebel SimBuilder версии 7.8.2, 7.8.5.

Опасность: Высокая.

Описание: 1. Уязвимость существует из-за недостаточной фильтрации параметров в пакетах SDO_GEOM, SDO_IDX и SDO_UTIL. Удаленный пользователь может выполнить произвольные SQL-команды в базе данных приложения.

2. Уязвимость существует из-за того, что пакет DBMS_STATS_INTERNAL сбрасывает пароль для OUTLN на значение по умолчанию и предоставляет пользователю OUTLN привилегии DBA на время создания вида.

3. Уязвимость существует из-за ошибки в функции flows_030000.www_execute_immediate.run_ddl(), входящей в состав Oracle Application Express. Удаленный пользователь может выполнить произвольные SQL-команды с повышенными привилегиями. Для успешной эксплуатации уязвимости требуется доступ к функции Oracle Application Express (по умолчанию учетные записи WMSYS, WKSYS, FLOWS_030000 и OUTLN). Подробности о других уязвимостях не сообщаются.

URL производителя: www.oracle.com.

Решение: Установите исправление с сайта производителя.

Переполнение буфера в Microsoft Windows GDI

Программа: Microsoft Windows 2000; Microsoft Windows 2000 Server; Microsoft Windows XP; Microsoft Windows Server 2003; Microsoft Windows Vista; Microsoft Windows Server 2008.

Опасность: Высокая.

Описание: 1. Уязвимость существует из-за ошибки в механизме подсчета целочисленных в GDI (Graphics Device Interface) при обработке заголовков графических файлов. Удаленный пользователь может с помощью EMF- или WMF-файла, содержащего специально сформированные значения заголовка (например, глубина цвета), вызвать переполнение динамической памяти и выполнить произвольный код на целевой системе.

2. Уязвимость существует из-за ошибки проверки границ данных в GDI при обработке параметров имени файла в EMF-файлах. Удаленный пользователь может с помощью специально сформированного EMF-файла вызвать переполнение стека и выполнить произвольный код на целевой системе.

URL производителя: www.microsoft.com.

Решение: Установите исправление с сайта производителя.

Множественные уязвимости в Adobe Flash Player

Программа: Adobe Flash Player версии до 9.0.124.0

Опасность: Высокая.

Описание: 1. Уязвимость существует из-за ошибки проверки границ данных при обработке тегов Declare Function (V7). Удаленный пользователь может с помощью специально сформированных флагов вызвать переполнение динамической памяти и выполнить произвольный код на целевой системе.

2. Целочисленное переполнение существует из-за ошибки при обработке мультимедийных файлов. Удаленный пользователь может вызвать переполнение буфера и выполнить произвольный код на целевой системе.

3. Уязвимость существует из-за ошибки при сопоставлении имени хоста IP-адресу. Удаленный пользователь может произвести DNS Rebinding-атаку. Подробное описание уязвимости: www.securitylab.ru/vulnerability/310072.php.

4. Уязвимость существует из-за ошибки при отправке HTTP-заголовков. Удаленный пользователь может обойти ограничения файлов междоменных политик.

5. Уязвимость существует из-за ошибки применения файлов междоменной политики. Злоумышленник может обойти некоторые ограничения безопасности на веб-серверах, размещающих междоменные файлы политик. Подробное описание уязвимости: www.securitylab.ru/vulnerability/310072.php.

6. Уязвимость существует из-за недостаточной обработки входных данных в некоторых параметрах в протоколе «asfunction:». Удаленный пользователь может с помощью специально сформированного запроса выполнить произвольный код сценария в браузере жертвы в контексте безопасности уязвимого сайта. Подробное описание уязвимости: www.securitylab.ru/vulnerability/310072.php.

URL производителя: www.adobe.com/products/flashplayer.

Решение: Установите последнюю версию с сайта производителя.

Переполнение буфера в Microsoft VBScript и JScript

Программа: Microsoft Windows 2000; Microsoft Windows 2000 Server; Microsoft Windows XP; Microsoft Windows Server 2003; Microsoft Windows Vista.

Опасность: Высокая.

Описание: Уязвимость существует из-за ошибки проверки границ данных в механизмах VBScript и JScript во время декодирования сценариев на веб-странице. Удаленный пользователь может с помощью специально сформированного веб-сайта вызвать переполнение буфера и выполнить произвольный код на целевой системе.

Примечание: Уязвимость не затрагивает системы с Internet Explorer 7.

URL производителя: www.microsoft.com.

Решение: Установите исправление с сайта производителя.

Составил Александр Антипов