

Переполнение буфера в Red Hat Directory Server

Программа: Red Hat Directory Server 7.x, 8.x.

Опасность: Средняя.

Описание: Уязвимость существует из-за ошибки проверки границ данных в обработке регулярных выражений. Удаленный пользователь может с помощью специально сформированного регулярного выражения в LDAP-поиске вызвать переполнение буфера и выполнить произвольный код на целевой системе.

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

Решение: Установите исправление с сайта производителя.

Уязвимость в реализации TCP/IP в Sun Solaris

Программа: Sun Solaris 8, 9, 10.

Опасность: Средняя.

Описание: Уязвимость существует из-за ошибки в реализации протокола TCP/IP. Удаленный пользователь может произвести TCP SYN Flood-атаку и потребить все доступные ресурсы процессора на системе. Для успешной эксплуатации уязвимости ndd(1M) tunable «tcp_conn_req_max_q0» должен быть установлен в значение выше 1024.

URL производителя: www.sun.com.

Решение: Установите исправление с сайта производителя.

Обход аутентификации в Oracle Application Server

Программа: Oracle Application Server 10g, возможно, другие версии.

Опасность: Средняя.

Описание: Уязвимость существует из-за того, что злоумышленник может обойти basic аутентификацию в Oracle Application Server Portal с помощью специально сформированного идентификатора сессии в файле куки, который устанавливается при доступе к /pls/portal/%0A. Удаленный пользователь может получить доступ к содержимому /dav/portal/portal/.

URL производителя: www.oracle.com/appserver.

Решение: В настоящее время способов устранения уязвимости не существует.

Утечка памяти в Cisco Catalyst Content Switching Module

Программа: CSM 4.2(3), 4.2(3a), 4.2(4), 4.2(5), 4.2(6), 4.2(7) и 4.2(8); CSM-S 2.1(2), 2.1(3), 2.1(4), 2.1(5), 2.1(6) и 2.1(7).

Опасность: Средняя.

Описание: Уязвимость существует из-за утечки памяти при обработке TCP-сегментов, содержащих определенные TCP-флаги. Удаленный пользователь может с помощью специально сформированного TCP-пакета вызвать отказ в обслуживании. Для удачной эксплуатации уязвимости на CSM или CSM-S должна быть сконфигурирована балансировка нагрузки на 7-м уровне.

URL производителя: www.cisco.com.

Решение: Установите последнюю версию CSM версии 4.2.9 или CSM-S версии 2.1.8 с сайта производителя.

Обход ограничений безопасности в Gentoo Linux

Программа: Gentoo Linux 1.x.

Опасность: Средняя.

Описание: Уязвимость существует из-за того, что сценарий /etc/conf.d/firebird устанавливает переменную окружения ISC_PASSWORD при запуске Firebird. Удаленный пользователь может, не указывая учетные данные, подключиться к СУБД с привилегиями SYSDBA.

URL производителя: www.gentoo.org.

Решение: Установите исправление с сайта производителя.

Обход ограничений безопасности в IBM WebSphere Application Server

Программа: IBM WebSphere Application Server 5.0.2.

Опасность: Средняя.

Описание: Уязвимость существует из-за неизвестной ошибки в Java-плагине. Удаленный пользователь может с помощью специально сформированного недоверенного апплета повысить свои привилегии на системе.

URL производителя: www.ibm.com.

Решение: Установите исправление APAR PK65161 с сайта производителя.

Несколько уязвимостей в Microsoft Malware Protection Engine

Программа: Microsoft Antigen 9.x; Microsoft Diagnostics and Recovery Toolset 6.x; Microsoft Forefront Client Security 1.x; Microsoft Forefront Security for Exchange Server; Microsoft Forefront Security for SharePoint; Microsoft Windows Defender; Microsoft Windows Live OneCare.

Опасность: Средняя.

Описание: 1. Уязвимость существует из-за неизвестной ошибки при обработке PE-файлов в Malware Protection Engine (MsMpEng.exe/mpengine.dll). Удаленный пользователь может с помощью специально сформированного файла вызвать отказ в обслуживании и перезапустить приложение.

2. Уязвимость существует из-за ошибки при обработке PE-файлов в Malware Protection Engine. Удаленный пользователь может с помощью PE-файла, содержащего специально сформированный размер заголовка, занять все доступное дисковое пространство в системе и вызвать отказ в обслуживании.

URL производителя: www.microsoft.com.

Решение: Установите исправление с сайта производителя.

Обход ограничений безопасности в Debian Linux и Ubuntu

Программа: Debian Linux 4.0; Ubuntu 7.04 (Feisty); Ubuntu 7.10 (Gutsy); Ubuntu 8.04 LTS (Hardy).

Опасность: Средняя.

Описание: Уязвимость существует из-за того, что OpenSSL использует предсказуемый генератор случайных чисел при создании ключей. Удаленный пользователь может получить доступ к зашифрованным данным.

Решение: Установите исправление с сайта производителя.

Составил Александр Антипов