

Переполнение буфера в IBM Lotus Domino Web Access Control ActiveX-компоненте

Программа: IBM Lotus Domino 6.x, IBM Lotus Domino 7.x, IBM Lotus Domino Web Access (iNotes) 6.x, IBM Lotus Domino Web Access 7.x.

Опасность: Критическая.

Описание: Уязвимость существует из-за ошибки проверки границ данных в dwa7.dwa7.1 ActiveX-компоненте (dwa7W.dll) при обработке строк, предназначенных для свойства «General_ServerName». Удаленный пользователь может с помощью специально сформированного веб-сайта передать методу InstallBrowserHelperDll() слишком длинную строку, вызвать переполнение стека и выполнить произвольный код на целевой системе.

URL производителя: www.ibm.com.

Решение: В настоящее время способов устранения уязвимости не существует.

Переполнение буфера в Cisco Unified Communications Manager

Программа: Cisco Unified CallManager 4.0, Cisco Unified CallManager 4.1 versions prior to 4.1(3)SR5c, Cisco Unified Communications Manager 4.2 versions prior to 4.2(3)SR3, Cisco Unified Communications Manager 4.3 versions prior to 4.3(1)SR1.

Опасность: Средняя.

Описание: Уязвимость существует из-за ошибки проверки границ данных в CTL Provider Service (CTLProvider.exe). Удаленный пользователь может отправить специально сформированный пакет на порт 2444/TCP, вызвать переполнение динамической памяти и выполнить произвольный код на целевой системе.

URL производителя: www.cisco.com.

Решение: Установите последнюю версию с сайта производителя.

Множественные уязвимости в PHP

Программа: PHP версии до 4.4.8.

Опасность: Средняя.

Описание: 1. Целочисленное переполнение буфера обнаружено в функции chunk_split().

2. Целочисленное переполнение обнаружено в функциях strcspn() и strspn().

3. Уязвимость существует из-за ошибки регрессии в функции glob(). Злоумышленник может обойти ограничения директивы open_basedir.

4. Уязвимость существует из-за ошибки при обработке SQL-запросов, содержащих LOCAL INFILE в MySQL-расширении. Злоумышленник может обойти ограничения директив open_basedir и safe_mode.

5. Уязвимость существует из-за ошибки при обработке значений переменных session_save_path и error_log. Злоумышленник может обойти ограничения директив open_basedir и safe_mode.

URL производителя: www.php.net.

Решение: Установите последнюю версию 4.4.8 с сайта производителя.

Уязвимость при обработке аутентификационных пакетов в McAfee E-Business Server

Программа: McAfee E-Business Server 8.5.2 и более ранние версии для Windows.

Опасность: Средняя.

Описание: Уязвимость существует из-за ошибки при обработке аутентификационных пакетов. Удаленный пользователь может вызвать отказ в обслуживании или выполнить произвольный код на целевой системе с привилегиями SYSTEM.

URL производителя: www.mcafee.com/us/smb/products/encryption/ebusiness_server.html.

Решение: Установите последнюю версию 8.5.3 с сайта производителя.

Отказ в обслуживании в Cisco PIX и ASA

Программа: Cisco Adaptive Security Appliance (ASA) 7.x, Cisco Adaptive Security Appliance (ASA) 8.x, Cisco PIX 7.x, Cisco PIX 8.x.

Опасность: Средняя.

Описание: Уязвимость существует из-за неизвестной ошибки при обработке IP-пакетов при включенном функционале уменьшения TTL (по умолчанию отключен). Удаленный пользователь может с помощью специально сформированного IP-пакета вызвать перезагрузку устройства.

URL производителя: www.cisco.com.

Решение: Установите последнюю версию 7.2(3)6, 8.0(3) или выше с сайта производителя.

Межсайтовый скриптинг в Sun Java System Web Server/Web Proxy Server

Программа: Sun Java System Web Proxy Server 3.x, Sun Java System Web Proxy Server 4.x, Sun Java System Web Server (Sun ONE/iPlanet) 6.x, Sun Java System Web Server 7.x.

Опасность: Низкая.

Описание: Уязвимость существует из-за недостаточной обработки входных данных. Удаленный пользователь может с помощью специально сформированного запроса выполнить произвольный код сценария в браузере жертвы в контексте безопасности уязвимого сайта.

URL производителя: www.sun.com.

Решение: Установите исправление с сайта производителя.

Отказ в обслуживании в OpenBSD

Программа: OpenBSD 4.2.

Опасность: Низкая.

Описание: Уязвимость существует из-за ошибки разыменования нулевого указателя при обработке SIOCGIFRTLABEL ioctl в файлах sys/net/if.c и sys/net/route.c. Злоумышленник может вызвать панику ядра системы с помощью специально сформированного SIOCGIFRTLABEL ioctl-вызова для интерфейсов, не содержащих метку маршрута.

URL производителя: www.openbsd.org.

Решение: Установите исправление с сайта производителя.

Составил Александр Антипов