

Отказ в обслуживании в Sun Java System Web Proxy Server

Программа: Sun Java System Web Proxy Server 4.x.

Опасность: Средняя.

Описание: Уязвимость существует из-за неизвестной ошибки в FTP-подсистеме. Удаленный пользователь может запретить прокси-серверу принимать новые подключения.

URL производителя: www.sun.com/software/products/web_proxy/home_web_proxy.xml.

Решение: Установите исправление с сайта производителя.

Несколько уязвимостей в Apache Tomcat

Программа: Apache Tomcat 4.1.37 и более ранние версии; Apache Tomcat 5.5.26 и более ранние версии; Apache Tomcat 6.0.16 и более ранние версии.

Опасность: Средняя.

Описание: 1. Уязвимость существует из-за недостаточной обработки входных данных в функции `HttpServlet Response.sendError()`, которые возвращаются в пользователю в HTTP-заголовке `Reason-Phrase`. Удаленный пользователь может с помощью специально сформированного запроса выполнить произвольный код сценария в браузере жертвы в контексте безопасности уязвимого сайта.

2. Уязвимость существует из-за того, что приложение нормализует целевой путь перед удалением строки запроса при использовании `RequestDispatcher`. Удаленный пользователь может получить возможность произвести обход каталога.

URL производителя: jakarta.apache.org/tomcat.

Решение: Установите исправление для версий 4.x, 5.x из SVN-репозитория или последнюю версию 6.0.18.

Целочисленное переполнение в ядре Linux

Программа: Linux kernel версии 2.6.17-rc1 и выше.

Опасность: Низкая.

Описание: Уязвимость существует из-за целочисленного переполнения в функции `dccp_setsockopt_change()` в файле `net/dccp/proto.c`. Локальный пользователь может вызвать панику ядра системы.

URL производителя: www.kernel.org.

Решение: Установите исправление из GIT-репозитория производителя.

Спуфинг атака в PowerDNS

Программа: PowerDNS версии до 2.9.21.1.

Опасность: Низкая.

Описание: Уязвимость существует из-за того, что сервер сбрасывает DNS-запросы к недействительным DNS-записям в пределах действительного домена. Злоумышленник может воспользоваться этим для проведения спуфинг-атаки на другой сервер.

URL производителя: www.powerdns.com.

Решение: Установите последнюю версию 2.9.21.1 с сайта производителя.

Уязвимость при обработке IPsec-политик в Microsoft Windows

Программа: Microsoft Windows 2008; Microsoft Windows Vista.

Опасность: Низкая.

Описание: Уязвимость существует из-за ошибки в механизме импорта IPsec-политик из доменов под управлением Windows Server 2003 в домены под управлением Windows Server 2008. В результате ошибки система игнорирует IPsec-политики и данные, которые должны быть зашифрованными, передаются в открытом виде.

URL производителя: www.microsoft.com.

Решение: Установите исправление с сайта производителя.

Раскрытие данных в VMware VirtualCenter

Программа: VMware VirtualCenter версии 2.0.2 до обновления Update 5 и 2.5 до обновления Update 2, возможно, другие версии

Опасность: Низкая.

Описание: Уязвимость существует из-за того, что служба VirtualCenter backend некорректно проверяет привилегии при выполнении некоторых действий. Удаленный пользователь может получить доступ к некоторым данным (например, именам системных учетных записей).

URL производителя: www.vmware.com/products/vi/vc.

Решение: Установите исправление с сайта производителя.

Отказ в обслуживании в Sun Solaris

Программа: Sun Solaris 10.

Опасность: Низкая.

Описание: Уязвимость существует из-за неизвестной ошибки, относящейся к системному вызову `sendfilev()`. Уязвимость может быть эксплуатирована локальным пользователем с помощью специально сформированного приложения, или удаленным пользователем с помощью специально сформированной веб-страницы, которая обслуживается веб-сервером Apache 2.2.x. Для успешной эксплуатации уязвимости с помощью веб-страницы, Apache должен быть собран без некоторых опций.

URL производителя: www.sun.com.

Решение: Установите исправление с сайта производителя.

Отказ в обслуживании в IPsec-Tools в rasoon

Программа: IPsec-Tools версии до 0.7.1.

Опасность: Низкая.

Описание: Уязвимость существует из-за утечки памяти в демоне rasoon при обработке некорректных предложений. Удаленный пользователь может вызвать отказ в обслуживании приложения.

URL производителя: ipsec-tools.sourceforge.net.

Решение: Установите последнюю версию 0.7.1 с сайта производителя.

Составил Александр Антипов