

Обход аутентификации в IBM WebSphere Portal Server

Программа: IBM WebSphere Portal Server версии 5.1.0.0, 5.1.0.1, 5.1.0.2, 5.1.0.3, 5.1.0.4, 5.1.0.5, 6.0.0.0, 6.0.0.1, 6.0.1.0, 6.0.1.1, 6.0.1.3 и 6.1.0.0.

Опасность: Средняя.

Описание: Уязвимость существует из-за того, что административный интерфейс недостаточно ограничивает доступ к некоторым страницам. Удаленный пользователь может с помощью специально сформированного HTTP-запроса произвести некоторые административные действия.

URL производителя: www-306.ibm.com/software/genservers/portal.

Решение: Установите последнюю версию 6.0.1.4 с сайта производителя.

Множественные уязвимости в Ruby

Программа: Ruby 1.8.5 и более ранние версии; Ruby 1.8.6-p286 и более ранние версии; Ruby 1.8.7-p71 и более ранние версии.

Опасность: Средняя.

Описание: 1. Множественные ошибки обнаружены в реализации ограничений безопасных уровней (safe level restrictions). Удаленный пользователь может вызвать функцию `untrace_var()`, произвести операции `syslog` и изменить `$PROGRAM_NAME` на безопасном уровне 4 или вызвать небезопасные методы на безопасных уровнях 1-3.

2. Уязвимость существует из-за использования регулярных выражений в `WEBrick::HTTPUtils.split_header_value()`. Удаленный пользователь может с помощью специально сформированного HTTP-запроса потребить все доступные ресурсы процессора на системе.

3. Уязвимость существует из-за ошибки в DL, которая позволяет удаленному пользователю обойти ограничения безопасности и выполнить потенциально опасные функции.

4. Уязвимость существует из-за того, что `resolv.rb` использует предсказуемый номер порта для DNS-запроса. Удаленный пользователь может отравить DNS-кэш.

URL производителя: www.ruby-lang.org/en.

Решение: Установите последнюю версию с сайта производителя.

Обход ограничений безопасности в Symantec Veritas Storage Foundation

Программа: Symantec Veritas Storage Foundation версии 5.0, 5.0 RP1a и 5.1.

Опасность: Средняя.

Описание: Уязвимость существует из-за того, что консоль управления позволяет NULL NTLMSSP-аутентификацию. Удаленный пользователь может обойти встроенный механизм аутентификации и добавит, удалить или изменить задачи по расписанию и скомпрометировать целевую систему.

URL производителя: www.symantec.com/enterprise/products/overview.jsp?pcid=1020&pvid=203_1.

Решение: Установите исправление с сайта производителя.

Несколько уязвимостей в продуктах CA

Программа: CA Host-Based Intrusion Prevention System (CA HIPS) 8.x; CA Internet Security Suite 2007; CA Internet Security Suite Plus 2008; CA Personal Firewall 2007; CA Personal Firewall 2008.

Опасность: Средняя.

Описание: 1. Уязвимость существует из-за ошибки при обработке IOCTL-запросов в драйвере ядра `kmxfw.sys`. Локальный пользователь может с помощью специально сформированного IOCTL-запроса аварийно завершить работу системы или выполнить произвольный код с привилегиями учетной записи SYSTEM.

2. Уязвимость существует из-за неизвестной ошибки в драйвере `kmxfw.sys`. Удаленный пользователь может произвести DoS-атаку.

URL производителя: www.ca.com.

Решение: Установите исправление с сайта производителя.

Множественные уязвимости в Python

Программа: Python версии 2.4.x, 2.5.x.

Опасность: Средняя.

Описание: 1. Целочисленные переполнения обнаружены в основных модулях `stringobject`, `unicodeobject`, `bufferobject`, `longobject`, `tupleobject`, `stropmodule`, `gcmodule` и `mmapmodule`.

2. Целочисленное переполнение обнаружено в `hashlib`-модуле, что может привести к ненадежным криптографическим результатам.

3. Целочисленное переполнение обнаружено при обработке Unicode-строк. Злоумышленник может вызвать переполнение буфера на 32-битной системе.

4. Целочисленное переполнение обнаружено в функции `PyOS_vsnprintf()` на архитектурах, которые не поддерживают функцию `vsnprintf()`.

5. Целочисленное переполнение обнаружено в функции `PyOS_vsnprintf()` при обработке строк нулевой длины. Злоумышленник может вызвать повреждение памяти.

URL производителя: python.org.

Решение: Установите исправление из SVN-репозитория производителя.

Выполнение произвольных команд в Sun Solaris

Программа: Sun Solaris 8, 9, 10.

Опасность: Средняя.

Описание: Уязвимость существует из-за неизвестной ошибки в сетевой утилите `snoor(1M)`, относящейся к отображению SMB-трафика. Удаленный пользователь может с помощью специально сформированного пакета, прочитанного или перехваченного приложением через опцию `-i`, выполнить произвольные команды на системе с привилегиями пользователя `snoor` или `nobody`. Для успешной эксплуатации уязвимости требуется, чтобы приложение было запущено без опции `-o`.

URL производителя: www.sun.com

Решение: Установите исправление с сайта производителя.

Составил Александр Антипов