

Отказ в обслуживании в ISC BIND для Windows

Программа: ISC BIND версии 9.3.5-P2-W1, BIND 9.4.2-P2-W1 и 9.5.0-P2-W1 для Windows.

Опасность: Средняя.

Описание: Уязвимость существует из-за ошибки при обработке UDP-пакетов. Удаленный пользователь может аварийно завершить работу клиентского UDP-обработчика.

Примечание: уязвимость не распространяется на UNIX-платформы.

URL производителя: www.isc.org/products/BIND.

Решение: Установите последнюю версию 9.3.5-P2-W2, 9.4.2-P2-W2 или 9.5.0-P2-W2 с сайта производителя.

Множественные уязвимости в Cisco Unity

Программа: Cisco Unity версии до 4.0ES161, 5.0ES53 и 7.0ES8.

Опасность: Низкая.

Описание: 1. Уязвимость существует из-за ошибки в процессе аутентификации в веб-интерфейсе. Когда злоумышленник запрашивает первый раз конфигурационную страницу, приложение перенаправляет пользователя на страницу аутентификации. Последующий запрос к этой же странице не будет перенаправлен, и удаленный неавторизованный пользователь сможет просмотреть и изменить некоторые конфигурационные данные.

2. Уязвимость существует из-за ошибки при обработке сессий. Удаленный пользователь может занять все доступные сессии и вызвать отказ в обслуживании. Для удачной эксплуатации уязвимости приложение должно быть сконфигурировано для анонимной аутентификации (не являясь значением по умолчанию).

3. Уязвимость существует из-за небезопасных привилегий на доступ к `\CommServer\Reports`. Пользователи домена могут получить доступ к некоторым важным данным.

URL производителя: www.cisco.com.

Решение: Установите последнюю версию 4.0ES161, 5.0ES53 или 7.0ES8 с сайта производителя.

Множественные уязвимости в Trend Micro OfficeScan

Программа: Trend Micro OfficeScan Corporate Edition 8.0.

Опасность: Средняя.

Описание: 1. Уязвимость существует в службе OfficeScanNT Listener. Удаленный пользователь может получить доступ к важным данным.

2. Уязвимость существует из-за неизвестных ошибок в CGI-модулях в OfficeScan-сервере. Удаленный пользователь может вызвать переполнение буфера и выполнить произвольный код на целевой системе.

3. Уязвимость существует из-за ошибки разыменования нулевого указателя в CGI-модулях в OfficeScan-сервере. Удаленный пользователь может с помощью специально сформированного HTTP-запроса вызвать отказ в обслуживании приложения.

URL производителя: www.trendmicro.com.

Решение: Установите исправление с сайта производителя.

Множественные уязвимости в Symantec Veritas NetBackup

Программа: Symantec Veritas NetBackup Server версии 5.1, 6.0 и 6.5; Symantec Veritas NetBackup Enterprise Server версии 5.1, 6.0 и 6.5.

Опасность: Средняя.

Описание: 1. Уязвимость существует из-за неизвестной ошибки в JAVA Administration GUI (jnbSA). Удаленный авторизованный пользователь с доступом к графическому интерфейсу может выполнить произвольные команды на системе с повышенными привилегиями.

2. Уязвимости существуют из-за ошибки проверки границ данных в `PVATLCalendar.PVCalendar.1` (`pvcalendar.ocx`) ActiveX-компоненте.

URL производителя: www.symantec.com.

Решение: Установите исправление с сайта производителя.

Повышение привилегий в Microsoft Windows

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

Опасность: Низкая.

Описание: 1. Уязвимость существует из-за ошибки при обработке свойств окна, передаваемых от родительского окна дочернему в процессе создания последнего. Локальный пользователь может выполнить произвольный код на целевой системе с повышенными привилегиями.

2. Уязвимость существует из-за ошибки двойного освобождения памяти при обработке системных вызовов от различных потоков. Локальный пользователь может выполнить произвольный код на целевой системе с повышенными привилегиями.

3. Уязвимость существует из-за недостаточной проверки входных данных, передаваемых их пользовательского режима в режим ядра. Локальный пользователь может выполнить произвольный код на целевой системе с повышенными привилегиями.

URL производителя: www.microsoft.com.

Решение: Установите исправление с сайта производителя.

Межсайтовый скриптинг в Cisco Unity

Программа: Cisco Unity 4.0ES161, 5.0ES53, 7.0ES8 и более ранние версии.

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.cisco.com.

Решение: В настоящее время способов устранения уязвимости не существует. Уязвимости будут исправлены в версиях 4.2(1)ES162 5.0(1)ES56 и 7.0(2)ES8.

Составил Александр Антипов