

Несколько уязвимостей в продуктах Symantec

Программа: Symantec AntiVirus for Network Attached Storage 4.3.16.39 и более ранние версии; Symantec AntiVirus Scan Engine 4.3.16.39 и более ранние версии; Symantec AntiVirus Scan Engine for Caching 4.3.16.39 и более ранние версии; Symantec AntiVirus Scan Engine for Clearswift 4.3.16.39 и более ранние версии; Symantec AntiVirus Scan Engine for Messaging 4.3.16.39 и более ранние версии; Symantec AntiVirus Scan Engine for MS ISA 4.3.16.39 и более ранние версии; Symantec AntiVirus Scan Engine for MS SharePoint 4.3.16.39 и более ранние версии; Symantec AntiVirus/Filtering for Domino MPE(AIX, Linux, Solaris); Symantec Mail Security for Microsoft Exchange 4.6.5.12 и более ранние версии; Symantec Mail Security for Microsoft Exchange 5.0.4.363 и более ранние версии; Symantec Scan Engine 5.1.4.24 и более ранние версии.

Опасность: Высокая.

Описание: 1. Уязвимость существует из-за ошибки проверки границ данных в механизме Symantec Decomposer. Удаленный пользователь может с помощью специально сформированного .RAR-файла вызвать переполнение стека и выполнить произвольный код на целевой системе.

2. Уязвимость существует из-за ошибки в механизме Symantec Decomposer. Удаленный пользователь может с помощью специально сформированного .RAR-файла заставить приложение потребить все доступные системные ресурсы.

URL производителя: www.symantec.com.

Решение: Установите исправление с сайта производителя.

Несколько уязвимостей в Symantec Backup Exec Calendar ActiveX-компоненте

Программа: Symantec Backup Exec for Windows Server 11d, 12.0

Опасность: Средняя.

Описание: 1. Два переполнения буфера обнаружены в PVATLCalendar.PVCalendar.1 (pvcalendar.ocx) ActiveX-компоненте при обработке строк, передаваемых различным свойствам (_DOWText0 в _DOWText6, _MonthText0 в _MonthText11). Удаленный пользователь может с помощью специально сформированного веб-сайта передать слишком длинные строки уязвимым свойствам и затем вызвать метод Save(). Удачная эксплуатация уязвимости позволит злоумышленнику вызвать переполнение стека и выполнить произвольный код на целевой системе.

2. Уязвимость существует из-за того, что PVATLCalendar.PVCalendar.1 (pvcalendar.ocx) ActiveX-компонент использует небезопасный метод Save(). Удаленный пользователь может с помощью специально сформированного веб-сайта перезаписать и повредить произвольные файлы на системе или записать злонамеренный сценарий в произвольную директорию на системе.

URL производителя: www.symantec.com/business/products/family.jsp?familyid=backupexec.

Решение: Установите исправление с сайта производителя.

Множественные уязвимости в Apache Tomcat

Программа: Apache Tomcat версии 5.5.0 по 5.5.25; Apache Tomcat версии 6.0.0 по 6.0.15; Apache Tomcat версии 4.1.0 по 4.1.36.

Опасность: Средняя.

Описание: 1. Уязвимость существует из-за ошибки в Native-соединителе (основанном на APR) при обработке SSL-запросов. Злоумышленник может вызвать повторную обработку последнего запроса путем подключения к SSL-порту и отключения без отправки данных.

Уязвимость присутствует в версиях с 5.5.11 по 5.5.25 и с 6.0.0 по 6.0.15.

2. Уязвимость существует из-за недостаточной обработки символа «%5C» в значениях куки. Удаленный пользователь может получить доступ к важным данным, включая идентификаторы сессий.

URL производителя: tomcat.apache.org.

Решение: Установите последнюю версию 5.5.26 или 6.0.16 с сайта производителя. Исправление для версий 4.x доступно в SVN-репозитории.

Множественные уязвимости в Opera

Программа: Opera версии до 9.26.

Опасность: Средняя.

Описание: 1. Уязвимость существует из-за ошибки дизайна при обработке данных в полях форм с типом «file». Злоумышленник может обманом заставить пользователя загрузить произвольные файлы на сервер.

2. Уязвимость существует из-за ошибки при обработке комментариев в свойстве изображения. Злоумышленник может с помощью специально сформированного комментария выполнить произвольный код сценария в браузере жертвы в неправильном контексте безопасности.

3. Уязвимость существует из-за ошибки при обработке значений атрибутов во время импорта XML-данных в документ. Злоумышленник может обойти фильтры и произвести XSS-нападение.

URL производителя: www.opera.com.

Решение: Установите последнюю версию 9.26 с сайта производителя.

Множественные уязвимости в Kerio MailServer

Программа: Kerio MailServer версии до 6.5.0.

Опасность: Средняя.

Описание: 1. Уязвимость существует из-за ошибки проверки границ данных в Visnetic anti-virus-плагине. Удаленный пользователь может вызвать переполнение буфера.

2. Уязвимость существует из-за ошибки во время uudecode-декодирования. Удаленный пользователь может вызвать повреждение памяти.

3. Уязвимость существует из-за наличия NULL DACL в AVG-плагине.

URL производителя: www.kerio.com/kms_home.html.

Решение: Установите последнюю версию 6.5.0 с сайта производителя.

Составил Александр Антипов