

Множественные уязвимости в Cisco Unified Communications Manager

Программа: Cisco Unified Communications Manager версии 4.1, 4.2, 4.3, 5.x и 6.x.

Опасность: Средняя.

Описание: 1. Уязвимость существует из-за ошибки в службе Certificate Trust List (CTL) Provider. Удаленный пользователь может отправить специально сформированный пакет на порт 2444/TCP и потребить большое количество системных ресурсов.

2. Уязвимость существует из-за ошибки в CTL Provider. Удаленный пользователь может отправить специально сформированный пакет на порт 2444/TCP и использовать все доступные ресурсы в системе. Уязвимости подвержены версии 5.x и 6.x.

3. Уязвимость существует из-за ошибки в Certificate Authority Proxy Function (CAPF). Удаленный пользователь может отправить специально сформированный пакет на порт 3804/TCP и вызвать отказ в обслуживании. Уязвимости подвержены версии 4.1, 4.2 и 4.3.

4. Уязвимость существует из-за ошибки при обработке SIP JOIN-сообщений. Удаленный пользователь с помощью специально сформированного SIP JOIN-сообщения может произвести DoS-атаку. Уязвимости подвержены версии 5.x и 6.x.

5. Уязвимость существует из-за ошибок при обработке SIP INVITE-сообщений. Удаленный пользователь может с помощью специально сформированного SIP INVITE-сообщения вызвать отказ в обслуживании. Уязвимость обнаружена в версиях 4.1, 4.2, 4.3, 5.x и 6.x.

6. Уязвимость существует из-за ошибки в SNMP Trap Agent. Удаленный пользователь может отправить специально сформированный UDP-пакет на порт 61441/UDP и вызвать отказ в обслуживании. Уязвимости подвержены версии 4.1, 4.2, 4.3, 5.x и 6.x.

URL производителя: www.cisco.com.

Решение: Установите исправление с сайта производителя.

Переполнение буфера в Novell Client

Программа: Novell Client for Windows NT/2000/XP 4.91 SP4, возможно, другие версии.

Опасность: Низкая.

Описание: Уязвимость существует из-за ошибки проверки границ данных в LOGINW32.DLL (4.19.6.0) при обработке имен пользователей и eDirectory «Context» строк в окне входа в систему в Novell Client. Локальный пользователь может с помощью слишком длинного имени пользователя или eDirectory «Context» строки, нажав на ссылку «Did you forget your password?», вызвать переполнение стека и выполнить произвольный код на системе в контексте процесса winlogon.exe.

URL производителя: www.novell.com/products/clients/windows/xp2000/overview.html.

Решение: В настоящее время способов устранения уязвимости не существует.

Множественные уязвимости в Symantec Altiris Deployment Solution

Программа: Symantec Altiris Deployment Solution версии до 6.9.176.

Опасность: Средняя.

Описание: 1. Уязвимость существует из-за недостаточной обработки входных данных в некоторых параметрах в ахengine.exe. Удаленный пользователь может выполнить произвольные SQL-команды в базе данных приложения и скомпрометировать целевую систему.

2. Уязвимость существует из-за неизвестной ошибки, которая позволяет запросить и получить без аутентификации зашифрованные личные данные Altiris Deployment Solution-домена.

3. Уязвимость существует из-за неизвестной ошибки, которая позволяет получить доступ к привилегированной командной строке посредством пользовательского интерфейса в Altiris Deployment Solution Agent.

4. Уязвимость существует из-за неизвестной ошибки, которая позволяет получить доступ к командной строке с привилегиями другого пользователя посредством GUI-элемента (tooltip).

5. Некоторые ключи реестра создаются с некорректными привилегиями. Злоумышленник может изменить или удалить эти ключи.

6. Уязвимость существует из-за некорректных привилегий на доступ к файлам в установочной директории приложения. Локальный пользователь может перезаписать файлы и выполнить произвольный код на системе с привилегиями администратора.

URL производителя: www.symantec.com.

Решение: Установите последнюю версию 6.9.176 с сайта производителя.

Множественные уязвимости в CA ARCserve Backup

Программа: CA ARCserve Backup r11.5 (formerly BrightStor ARCserve Backup r11.5); CA ARCserve Backup r11.1 (formerly BrightStor ARCserve Backup r11.1); CA ARCserve Backup r11.0 (formerly BrightStor ARCserve Backup r11.0); CA Server Protection Suite r2; CA Business Protection Suite r2; CA Business Protection Suite for Microsoft Small Business Server Standard Edition r2; CA Business Protection Suite for Microsoft Small Business Server Premium Edition r2.

Опасность: Средняя.

Описание: 1. Уязвимость существует из-за ошибки проверки входных данных в службе журналирования (caloggerd). Удаленный пользователь может с помощью символов обхода каталога добавить произвольные данные в произвольные файлы на системе.

2. Уязвимость существует из-за ошибок проверки границ данных в xdr функциях (например, xdr_rwsstring()). Удаленный пользователь может вызвать переполнение стека и выполнить произвольный код на целевой системе.

URL производителя: www.ca.com.

Решение: Установите исправление с сайта производителя.

Составил Александр Антипов