

Несколько уязвимостей в Red Hat Directory Server

Программа: Red Hat Directory Server 8.x.

Опасность: Средняя.

Описание: 1. Уязвимость существует из-за недостаточной обработки входных данных в repl-monitor.cgi.pl CGI-сценарии перед вызовом функции system(). Удаленный пользователь с доступом к странице «replication monitor» может выполнить произвольные команды на системе с привилегиями Administration Server (по умолчанию «nobody»).

2. Уязвимость существует из-за недостаточного ограничения доступа к некоторым сценариям. Удаленный пользователь может получить доступ к важным данным или произвести некоторые запрещенные действия. Для успешной эксплуатации уязвимости требуется доступ к порту Administration Server 9830/TCP.

URL производителя: www.redhat.com.

Решение: Установите исправление с сайта производителя.

Выполнение произвольных команд в Cisco Unified Communications Disaster Recovery Framework

Программа: Cisco Unified Communications Manager (CUCM) 5.x и 6.x; Cisco Unified Communications Manager Business Edition; Cisco Unified Precense 1.x и 6.x; Cisco Emergency Responder 2.x; Cisco Mobility Manager 2.x.

Опасность: Средняя.

Описание: Уязвимость существует из-за того, что Disaster Recovery Framework (RDF) Master-сервер не производит аутентификацию запросов, полученных по сети. Удаленный пользователь может с помощью специально сформированного запроса удалить или изменить запланированное резервное копирование данных, скопировать резервную копию на удаленную систему, восстановить произвольную конфигурацию с удаленного сервера и выполнить произвольные команды с административными привилегиями.

URL производителя: www.cisco.com.

Решение: Установите исправление с сайта производителя.

Отказ в обслуживании в Asterisk

Программа: Asterisk Open Source 1.0.x (все версии); Asterisk Open Source 1.2.x (версии до 1.2.28); Asterisk Open Source 1.4.x (версии до 1.4.19.1); Asterisk Business Edition A.x.x (все версии); Asterisk Business Edition B.x.x (версии до B.2.5.2); Asterisk Business Edition C.x.x (версии до C.1.8.1); AsteriskNOW 1.0.x (версии до 1.0.3); Asterisk Appliance Developer Kit 0.x.x (все версии); s800i (Asterisk Appliance) 1.0.x (версии до 1.1.0.3).

Опасность: Средняя.

Описание: Уязвимость существует из-за некорректной проверки АСК-ответов во время IAX2-рукопожатий. Злоумышленник может произвести подмену IAX2-рукопожатия и вызвать отказ в обслуживании за счет потребления всей пропускной способности.

URL производителя: www.asterisk.org.

Решение: Установите последнюю версию с сайта производителя.

Отказ в обслуживании в Sun Solaris

Программа: Sun Solaris 8,9, 10.

Опасность: Низкая.

Описание: Уязвимость существует из-за неизвестной ошибки при обработке самоинкапсулирующихся IP-пакетов. Удаленный пользователь может с помощью специально сформированного IP-пакета аварийно завершить работу целевой системы.

URL производителя: www.sun.com.

Решение: Установите исправление с сайта производителя.

Множественные уязвимости в продуктах CA

Программа: CA Anti-Virus for Enterprise 7.1; CA Threat Manager for Enterprise (панель eTrust Integrated Threat Management) r8; CA Threat Manager for Enterprise (панель eTrust Integrated Threat Management) r8.1; CA Anti-Virus for Enterprise (панель eTrust Antivirus) r8; CA Anti-Virus for Enterprise (панель eTrust Antivirus) r8.1; BrightStor ARCserve Backup r11.5; BrightStor ARCserve Backup r11.1; BrightStor ARCserve Backup r11 for Windows.

Опасность: Низкая.

Описание: Уязвимости существуют из-за ошибок проверки границ данных в службе CA Alert Notification Server. Удаленный авторизованный пользователь может вызвать отказ в обслуживании или выполнить произвольный код на целевой системе.

URL производителя: www.ca.com.

Решение: Установите исправление с сайта производителя.

Раскрытие данных в Cisco Network Admission Control

Программа: Cisco Clean Access (CCA) версии до 3.6.4.4; Cisco NAC Appliance версии 4.0.x до 4.0.6 и 4.1.x до 4.1.2.

Опасность: Средняя.

Описание: Уязвимость существует из-за неизвестной ошибки, которая позволяет удаленному пользователю получить доступ к общему паролю, который используется в CAS и CAM, передаваемому в лог-файлах по локальной сети.

URL производителя: www.cisco.com.

Решение: Установите последнюю версию 3.6.4.4, 4.0.6 или 4.1.2 с сайта производителя.

Повышение привилегий в Red Hat Enterprise Linux

Программа: Red Hat Enterprise Linux (v. 5 server); Red Hat Enterprise Linux Desktop (v. 5 client); Red Hat Enterprise Linux Desktop Workstation (v. 5 client).

Опасность: Низкая.

Описание: Уязвимость существует из-за ошибки в сценарии capp-lspg-config, которая делает сценарий «/etc/pam.d/system-auth» доступным для записи всем пользователям. Локальный пользователь может повысить свои привилегии на системе.

URL производителя: www.redhat.com.

Решение: Установите исправление с сайта производителя.

Составил Александр Антипов