

## Раскрытие данных в ядре Linux

**Программа:** Linux kernel версии до 2.6.27-rc2.

**Опасность:** Низкая.

**Описание:** Уязвимость существует из-за ошибки в функции `snd_seq_oss_synth_make_info()` в файле `sound/core/seq/oss/seq_oss_synth.c`. Локальный пользователь может передать некорректный номер устройства уязвимой функции и получить доступ к потенциально важным данным.

**URL производителя:** [www.kernel.org](http://www.kernel.org).

**Решение:** Установите последнюю версию 2.6.27-rc2 с сайта производителя.

## Повышение привилегий в Sun Solaris

**Программа:** Sun Solaris 8, 9, 10.

**Опасность:** Низкая.

**Описание:** Уязвимость существует из-за неизвестной ошибки в модуле ядра `namefs`. Локальный пользователь может вызвать панику ядра системы или выполнить произвольный код в контексте ядра.

**URL производителя:** [www.sun.com](http://www.sun.com).

**Решение:** Установите исправление с сайта производителя.

## Переполнение буфера в ядре Linux

**Программа:** Linux kernel версии до 2.6.25.11.

**Опасность:** Низкая.

**Описание:** Уязвимость существует из-за ошибки при обработке размера LDT-буфера на x86\_64-системах. Локальный пользователь может вызвать отказ в обслуживании или выполнить произвольный код на целевой системе с привилегиями учетной записи `root`.

**URL производителя:** [www.kernel.org](http://www.kernel.org).

**Решение:** Установите последнюю версию 2.6.25.11 с сайта производителя.

## Выполнение произвольного кода в CA ARCserve Backup for Laptops and Desktops

**Программа:** CA ARCserve Backup for Laptops and Desktops r11.5; CA ARCserve Backup for Laptops and Desktops r11.1 SP2; CA ARCserve Backup for Laptops and Desktops r11.1 SP1; CA ARCserve Backup for Laptops and Desktops r11.1; CA ARCserve Backup for Laptops and Desktops r11.0; CA Desktop Management Suite 11.2; CA Desktop Management Suite 11.1; CA Protection Suites r2; CA Protection Suites 3.0; CA Protection Suites 3.1.

**Опасность:** Средняя.

**Описание:** Уязвимость существует из-за ошибки потери значимости целочисленных в службе `LGServer` при обработке входящих сообщений. Удаленный пользователь может отправить специально сформированное сообщение службе `LGServer` на порт 1900/TCP, вызвать переполнение буфера и выполнить произвольный код на целевой системе.

**URL производителя:** [www.ca.com/us/products/product.aspx?id=263](http://www.ca.com/us/products/product.aspx?id=263).

**Решение:** Установите исправление с сайта производителя.

## Межсайтовый скриптинг в Apache mod\_proxy\_ftp

**Программа:** Apache 2.0.63 и 2.2.9, возможно более ранние версии.

**Опасность:** Низкая.

**Описание:** Уязвимость существует из-за недостаточной обработки входных данных в URL, содержащих символ «\*» в модуле `mod_proxy_ftp`. Удаленный пользователь может с помощью специально сформированного запроса выполнить произвольный код сценария в браузере жертвы в контексте безопасности уязвимого сайта.

**URL производителя:** [www.apache.org](http://www.apache.org).

**Решение:** Установите исправление из SVN-репозитория производителя.

## Раскрытие данных в OpenSSH

**Программа:** OpenSSH версии до 5.1.

**Опасность:** Низкая.

**Описание:** Уязвимость существует из-за того, что `sshd`-сервер устанавливает опцию `SO_REUSEADDR` для прослушивания сокета, используемого перенаправляющим X11-сервером. Локальный пользователь может подключиться к X11 перенаправляющему порту и перехватить X11-сессию. Для успешной эксплуатации уязвимости опция `X11UseLocalhost` должна быть отключена (по умолчанию включена) и операционная система должна позволять повторное подключение к порту без проверки идентификатора пользователя или IP-адреса (например, HP/UX).

**URL производителя:** [openssh.com](http://openssh.com).

**Решение:** Установите последнюю версию 5.1 или 5.1p1 с сайта производителя.

## Отказ в обслуживании в Asterisk

**Программа:** Asterisk Open Source 1.0.x (все версии); Asterisk Open Source 1.2.x (все версии до 1.2.30); Asterisk Open Source 1.4.x (все версии до 1.4.21.2); Asterisk Business Edition A.x.x (все версии); Asterisk Business Edition B.x.x.x (все версии до B.2.5.4); Asterisk Business Edition C.x.x.x (все версии до C.1.10.3); AsteriskNOW pre-release (все версии); Asterisk Appliance Developer Kit 0.x.x (все версии); s800i (Asterisk Appliance) 1.0.x (все версии до 1.2.0.1).

**Опасность:** Низкая.

**Описание:** 1. Уязвимость существует из-за ошибки при обработке IAX2 POKE-запросов. Удаленный пользователь может отправить большое количество POKE-запросов, не отправляя ACK-пакет в ответ на пакет PONG, и потребить все IAX2-номера.

2. Уязвимость существует из-за того, что протокол загрузки прошивки не требует рукопожатия. Удаленный пользователь может отправить произвольном серверу пакеты размером 1040 байта с помощью 40-байтного пакета с подмененным адресом источника.

**URL производителя:** [www.asterisk.org](http://www.asterisk.org).

**Решение:** Установите последнюю версию с сайта производителя.

Составил Александр Антипов