

## Переполнение буфера в ядре Linux

**Программа:** Linux kernel версии до 2.6.25.5 и 2.4.36.6.

**Опасность:** Средняя.

**Описание:** Уязвимость существует из-за ошибки проверки границ данных в модулях `ip_nat_snmp_basic` и `cifs` в ASN.1 BER декодере. Удаленный пользователь может с помощью специально сформированных BER-кодированных данных вызвать отказ в обслуживании или скомпрометировать целевую систему.

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

**Решение:** Установите последнюю версию ядра 2.6.25.5 или 2.4.36.6 с сайта производителя.

## Множественные уязвимости в Cisco ASA и PIX

**Программа:** Cisco Adaptive Security Appliance (ASA) 7.x, 8.x; Cisco PIX 7.x, 8.x.

**Опасность:** Средняя.

**Описание:** 1. Уязвимость существует из-за неизвестной ошибки при обработке TCP ACK-пакетов. Удаленный пользователь может с помощью специально сформированного пакета вызвать отказ в обслуживании устройства. Уязвимости подвержены версии 7.1.x, 7.2.x и 8.0.x.

2. Уязвимость существует из-за неизвестной ошибки при обработке TLS-протокола. Удаленный пользователь может с помощью специально сформированного TLS-пакета вызвать перезагрузку устройства. Уязвимости подвержены версии 8.0.x и 8.1.x.

3. Уязвимость существует из-за неизвестной ошибки в Instant Messaging Inspection. Удаленный пользователь может вызвать отказ в обслуживании устройства. Для успешной эксплуатации уязвимости Instant Messaging Inspection должен быть включен. Уязвимости подвержены версии 7.2.x, 8.0.x и 8.1.x.

4. Уязвимость существует из-за неизвестной ошибки, которая позволяет вызвать перезагрузку устройства посредством специально сформированного трафика (например, с помощью сканера уязвимостей/портов) на порт 443/TCP.

5. Уязвимость существует из-за неизвестной ошибки, которая приводит к некорректной работе списков контроля доступа. Удаленный пользователь может обойти ограничения ACL. Уязвимости подвержены версии 8.0.x.

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

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

## Отказ в обслуживании в Apache mod\_proxy

**Программа:** Apache 2.2.8 и 2.0.63, возможно, более ранние версии.

**Опасность:** Низкая.

**Описание:** Уязвимость существует из-за ошибки в функции `ap_proxy_http_process_response()` при перенаправлении промежуточных ответов. Удаленный пользователь может заставить модуль `mod_proxy` отправить большое количество промежуточных ответов клиенту и потребить большое количество памяти на системе.

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

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

## Множественные уязвимости в Cisco Service Control Engine

**Программа:** Cisco Service Control Engine 1000; Cisco Service Control Engine 2000.

**Опасность:** Средняя.

**Описание:** 1. Уязвимость существует из-за ошибки при обработке попыток авторизации на SCE SSH-сервере. Удаленный пользователь может создать большое количество подключений и вызвать нестабильную работу устройства или перезагрузку. Уязвимость существует в SCE 1000 и 2000 в версиях до 3.1.6.

2. Уязвимость существует из-за наличия некорректных операций ввода/вывода при обработке легитимного SSH-трафика на SCE-интерфейсе управления совместно с некоторыми задачами по управлению. Удаленный пользователь может вызвать отказ в обслуживании устройства. Уязвимость существует в SCE 1000 и 2000 в версиях до 3.0.7 и 3.1.0.

3. Уязвимость существует из-за ошибки в процессе авторизации в SCE SSH-сервере, которая не связана с частотой попыток входа или другими задачами. Злоумышленник может попытаться использовать определенные учетные данные для попытки смены метода аутентификации, что может сказаться на производительности системы. Уязвимость существует в SCE 1000 и 2000 в версиях до 3.1.6.

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

**Решение:** Установите исправление с сайта производителя, доступное для зарегистрированных клиентов.

## Выполнение произвольного кода в ядре Linux

**Программа:** Linux kernel 2.6.18, возможно, другие версии.

**Опасность:** Средняя.

**Описание:** Уязвимость существует из-за недостаточной проверки входных данных в функции `dccp_feat_change()` файла `net/dccp/feat.c` в подсистеме DCCP (Datagram Congestion Control Protocol). Удаленный пользователь может вызвать переполнение буфера и выполнить произвольный код на целевой системе.

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

**Решение:** В настоящее время способов устранения уязвимости не существует. Некоторые производители Linux-систем выпустили исправления.

## Спуфинг-атака в Net-SNMP

**Программа:** Net-SNMP версии до 5.4.1.1, 5.3.2.1 и 5.2.4.1.

**Опасность:** Низкая.

**Описание:** Уязвимость существует из-за ошибки при проверке подлинности HMAC-дайджеста. Удаленный пользователь может с помощью специально сформированного SNMPv3-пакета, с неполным однобайтным HMAC-дайджестом, увеличить возможность удачной подмены до 1 из 256 пакетов.

**URL производителя:** [net-snmp.sourceforge.net](http://net-snmp.sourceforge.net).

**Решение:** Установите последнюю версию 5.4.1.1, 5.3.2.1 или 5.2.4.1 с сайта производителя.

Составил Александр Антипов