

## Обход ограничений безопасности в Apache Tomcat

**Программа:** Apache Tomcat версии 4.1.0 по 4.1.31; Apache Tomcat версия 5.5.0.

**Опасность:** Низкая.

**Описание:** Уязвимость существует из-за ошибки синхронизации при проверке IP-адресов. Удаленный пользователь может обойти ограничения фильтра и получить доступ к защищенным данным с заблокированного IP-адреса.

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

**Решение:** Установите последнюю версию 4.1.32 или 5.5.1 с сайта производителя.

## Небезопасная обработка временных файлов в FreeRADIUS

**Программа:** FreeRADIUS 2.0.4, возможно, более ранние версии.

**Опасность:** Низкая.

**Описание:** Уязвимость существует из-за того, что сценарии `dialup_admin/bin/backup_radacct`, `dialup_admin/bin/clean_radacct`, `dialup_admin/bin/monthly_tot_stats`, `dialup_admin/bin/tot_stats` и `dialup_admin/bin/truncate_radacct` небезопасным образом обрабатывают временные файлы. Локальный пользователь может с помощью специально сформированной символической ссылки перезаписать произвольные файлы на системе с повышенными привилегиями.

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

**Решение:** В настоящее время способов устранения уязвимости не существует.

## Повышение привилегий в Gentoo Linux

**Программа:** Gentoo Linux 1.x.

**Опасность:** Низкая.

**Описание:** Уязвимость существует из-за того, что системная утилита `portage` (версии до 2.1.4.5) включает текущую рабочую директорию в путь модуля поиска. Злоумышленник может поместить злонамеренный модуль, например, в директорию `/tmp` и обманом заставить администратора произвести `emerge` из этой директории для определенных пакетов (например, `sys-apps/portage`, `net-mail/fetchmail` или `app-editors/leo`). Успешная эксплуатация уязвимости позволит злоумышленнику повысить свои привилегии на системе.

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

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

## Обход ограничений безопасности в ModSecurity

**Программа:** ModSecurity версии 2.5.0 по 2.5.5.

**Опасность:** Низкая.

**Описание:** Уязвимость существует из-за ошибки в механизме кеширования трансформаций. Удаленный пользователь может в некоторых случаях обойти проверку ModSecurity. Для успешной эксплуатации уязвимости опция `SecCacheTransformations` должна быть включена.

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

**Решение:** Установите последнюю версию 2.5.6 с сайта производителя.

## Уязвимость в протоколе IPv6 Neighbor Discovery в продуктах Juniper

**Программа:** Juniper IVE OS Software 1.x; Juniper IVE OS Software 2.x; Juniper IVE OS Software 3.x; Juniper IVE OS Software 4.x; Juniper IVE OS Software 5.x; Juniper IVE OS Software 6.x; Juniper Networks DXOS 5.x; Juniper Networks IDP 4.x; Juniper Networks Infranet Controller 4000; Juniper Networks Infranet Controller 6000; Juniper Networks Secure Access 2000; Juniper Networks Secure Access 4000 (NetScreen-SA 3000 Series); Juniper Networks Secure Access 6000 (NetScreen-SA 5000 Series); Juniper Networks Secure Access 6000 SP; Juniper Networks Secure Access 700; Juniper Networks Session and Resource Control (SRC) 1.x; Juniper Networks Session and Resource Control (SRC) 2.x; Juniper Networks WX Series; Juniper Networks WXC Series.

**Опасность:** Низкая.

**Описание:** Уязвимость существует из-за ошибки в реализации Neighbor Discovery протокола при обработке запросов на опрос соседа (`neighbor solicitation`). Удаленный пользователь может с помощью опроса соседа, содержащего поддельный IPv6-адрес, добавить этот адрес в таблицу кеша соседа и перехватить или помешать передаче сетевого трафика. Для успешной эксплуатации уязвимости, IPv6-узлы, участвующие в атаке, должны использовать один и тот же маршрутизатор.

**URL производителя:** [www.juniper.net](http://www.juniper.net).

**Решение:** В настоящее время способов устранения уязвимости не существует.

## Повышение привилегий в ядре Linux

**Программа:** Linux kernel 2.6.x.

**Опасность:** Низкая.

**Описание:** Уязвимость существует из-за ошибки в функции `vmi_write_ldt_entry()` в `arch/x86/kernel/vmi_32.c`. Локальный пользователь может с помощью функции `sys_modify_ldt()` записать значения в IDT и повысить свои привилегии на системе. Для успешной эксплуатации уязвимости ядро должно быть запущено как VMI-гость на x86-системе.

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

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

## Повышение привилегий в Virtual Address Descriptor в Microsoft Windows

**Программа:** Microsoft Windows XP, Microsoft Windows Server 2003, Microsoft Windows Vista, Microsoft Windows Server 2008.

**Опасность:** Низкая.

**Описание:** Целочисленное переполнение обнаружено при обработке параметров VAD (Virtual Address Descriptor). Локальный пользователь может вызвать повреждение памяти и выполнить произвольный код на целевой системе с повышенными привилегиями.

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

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

Составил Александр Антипов