

## Переполнение буфера в Novell GroupWise

**Программа:** Novell GroupWise 6.5.6, возможно, более ранние версии.

**Опасность:** Высокая.

**Описание:** Уязвимость существует из-за ошибки проверки границ данных при обработке e-mail-сообщений. Удаленный пользователь может с помощью специально сформированного HTML-сообщения, содержащего слишком длинный SRC-параметр в теге IMG, вызвать переполнение стека и выполнить произвольный код на целевой системе. Для успешной эксплуатации уязвимости требуется, чтобы опция предварительного просмотра в HTML-виде была включена и пользователь ответил или переслал специально сформированное e-mail-сообщение.

**URL производителя:** [www.novell.com/products/groupwise](http://www.novell.com/products/groupwise).

**Решение:** Установите последнюю версию 6.5.7 с сайта производителя.

## Множественные уязвимости в yaSSL

**Программа:** yaSSL Library 1.7.5, возможно, более ранние версии.

**Опасность:** Высокая.

**Описание:** 1. Уязвимость существует из-за ошибки проверки границ данных в методе ProcessOldClientHello() в файле src/handshake.cpp. Удаленный пользователь может с помощью специально сформированного SSLv2 «Hello»-пакета вызвать переполнение стека и выполнить произвольный код на целевой системе.

2. Уязвимость существует из-за ошибки проверки границ данных в реализации входного оператора для SSL «Hello»-пакетов в файле src/yaSSL\_imp.cpp. Удаленный пользователь может с помощью специально сформированного SSLv3 «Hello»-пакета вызвать переполнение стека и выполнить произвольный код на целевой системе.

3. Уязвимость существует из-за ошибки проверки границ данных в методе HASHwithTransform::Update() в файле taocrypt/src/hash.cpp. Удаленный пользователь может с помощью специально сформированного SSL «Hello»-пакета вызвать отказ в обслуживании приложения.

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

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

## Переполнение буфера в Microsoft Visual InterDev

**Программа:** Microsoft Visual InterDev 6.0 (SP6), возможно, более ранние версии.

**Опасность:** Средняя.

**Описание:** Уязвимость существует из-за ошибки проверки границ данных при обработке .sln-файлов. Удаленный пользователь может с помощью специально сформированного .sln-файла, содержащего слишком длинное поле «Project», вызвать переполнение буфера и выполнить произвольный код на целевой системе.

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

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

## Уязвимость в реализации TCP/IP в Microsoft Windows

**Программа:** Microsoft Windows 2000, Microsoft Windows XP, Microsoft Windows 2003, Microsoft Windows Vista.

**Опасность:** Средняя.

**Описание:** 1. Уязвимость существует из-за ошибки в реализации TCP/IP в драйвере tcpip.sys при обработке IGMPv3- и MLDv2-запросов. Удаленный пользователь может с помощью специально сформированного IGMPv3- или MLDv2-пакета аварийно завершить работу системы или выполнить произвольный код. Эта уязвимость не распространяется на системы под управлением Windows 2000.

2. Уязвимость существует из-за ошибки в реализации TCP/IP в драйвере tcpip.sys при обработке фрагментированных ICMP-анонсов маршрутизатора. Удаленный пользователь может с помощью специально сформированного ICMP-запроса вызвать отказ в обслуживании системы. Для успешной эксплуатации уязвимости протокол Router Discovery Protocol (RDP) должен быть включен (по умолчанию отключен). Эта уязвимость не распространяется на системы под управлением Windows Vista.

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

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

## Множественные уязвимости в Mambo

**Программа:** Mambo 4.6.2 и более ранние версии.

**Опасность:** Высокая.

**Описание:** 1. Уязвимость существует из-за использования уязвимой версии PHPMailer.

2. Уязвимость существует из-за недостаточной обработки входных данных. Удаленный пользователь может с помощью специально сформированного запроса выполнить произвольный код сценария в браузере жертвы в контексте безопасности уязвимого сайта.

3. Уязвимость существует из-за неизвестной ошибки в функционале выбора шаблонов. Подробности уязвимости не сообщаются.

**URL производителя:** [www.mambo-foundation.org](http://www.mambo-foundation.org).

**Решение:** Установите последнюю версию 4.6.3 с сайта производителя.

## Отказ в обслуживании в Cisco Firewall Services Module

**Программа:** Cisco Firewall Services Module (FWSM) 3.2(3).

**Опасность:** Средняя.

**Описание:** Уязвимость существует из-за неизвестной ошибки при обработке данных в control-plane для Layer 7 Application Inspections при нормализации TCP-трафика. Удаленный пользователь может с помощью специально сформированных данных вызвать отказ в обслуживании или перезагрузку FWSM.

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

**Решение:** Для устранения уязвимости следуйте инструкциям производителя.

Составил Александр Антипов