

## Множественные уязвимости в Sun Java System Active Server Pages

**Программа:** Sun Java System Active Server Pages 4.0.2, возможно, более ранние версии.

**Опасность:** Высокая.

**Описание:** 1. Уязвимость существует из-за того, что неизвестный файл, который подключается в различных ASP-приложениях, недостаточно проверяет входные данные перед созданием файлов на системе. Удаленный пользователь может создать и изменить произвольные файлы на системе. Для успешной эксплуатации уязвимости требуется доступ к административному серверу (порт 5100/TCP).

2. Уязвимость существует из-за того, что пароли и конфигурационные данные хранятся в корневой директории веб-сервера. Удаленный пользователь может получить доступ к потенциально важным данным, включая хеши паролей пользователей. Для успешной эксплуатации уязвимости требуется доступ к административному серверу (порт 5100/TCP).

3. Уязвимость существует из-за недостаточной обработки входных данных в некоторых ASP-приложениях. Удаленный пользователь может с помощью специально сформированного HTTP-запроса, содержащего символы обхода каталога, просмотреть или удалить произвольные файлы на системе. Для успешной эксплуатации уязвимости требуется доступ к административному серверу (порт 5100/TCP).

4. Уязвимость существует из-за ошибки проверки границ данных при обработке запросов в ASP-сервере. Удаленный пользователь может с помощью специально сформированного запроса вызвать переполнение стека и выполнить произвольный код на целевой системе.

5. Уязвимость существует из-за недостаточной обработки входных данных в некоторых ASP-приложениях. Удаленный пользователь может с помощью специально сформированного HTTP-запроса, содержащего метасимволы, выполнить произвольные команды на системе. Для успешной эксплуатации уязвимости требуется административный доступ к приложению.

6. Уязвимость существует из-за ошибки дизайна при обработке аутентификации. Удаленный пользователь может отправить специально сформированные запросы на порт 5102/TCP и обойти процесс аутентификации.

**URL производителя:** [www.sun.com/software/chilisoft/index.xml](http://www.sun.com/software/chilisoft/index.xml).

**Решение:** Установите последнюю версию 4.0.3 с сайта производителя.

## Уязвимость в реализации Secure Shell в Cisco IOS

**Программа:** Cisco IOS 12.4.

**Опасность:** Средняя.

**Описание:** Множественные уязвимости существуют из-за ошибок в реализации SSH. Удаленный пользователь может вызвать перезагрузку устройства.

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

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

## Множественные уязвимости в GnuTLS

**Программа:** GnuTLS версии до 2.2.4.

**Опасность:** Высокая.

**Описание:** 1. Уязвимость существует из-за ошибки проверки границ данных при обработке сообщений «Client Hello», содержащих расширение Server Name. Удаленный пользователь может с помощью специально сформированного TLS-пакета вызвать переполнение динамической памяти и выполнить произвольный код на целевой системе.

2. Уязвимость существует из-за ошибки разыменования нулевого указателя при обработке TLS-пакетов, содержащих большое количество сообщений «Client Hello». Удаленный пользователь может с помощью специально сформированного TLS-пакета аварийно завершить работу приложения.

3. Уязвимость существует из-за ошибки при обработке знаковых переменных в функции `_gnutls_ciphertext2_compressed()` в файле `lib/gnutls_cipher.c`. Удаленный пользователь может с помощью специально сформированных TLS-данных вызвать переполнение буфера и аварийно завершить работу приложения.

**URL производителя:** [www.gnu.org/software/gnutls](http://www.gnu.org/software/gnutls).

**Решение:** Установите последнюю версию 2.2.5 с сайта производителя.

## Переполнение буфера в Samba

**Программа:** Samba 3.0.29 и более ранние версии.

**Опасность:** Высокая.

**Описание:** Уязвимость существует из-за ошибки проверки границ данных при обработке SMB-пакетов в функции `receive_smb_raw()` в файле `lib/util_sock.c`. Удаленный пользователь может с помощью слишком длинного SMB-пакета вызвать переполнение динамической памяти и выполнить произвольный код на целевой системе. Для успешной эксплуатации уязвимости злоумышленник должен обманом заставить пользователя подключиться к злонамеренному серверу (нажать на ссылку типа «`smb://`») или отправить специально сформированные пакеты демону `nmbd`, сконфигурированному как основной браузер домена.

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

**Решение:** Установите последнюю версию 3.0.30 с сайта производителя.

## Переполнение буфера в IBM Lotus Sametime

**Программа:** IBM Lotus Sametime 7.5.1

**Опасность:** Высокая.

**Описание:** Уязвимость существует из-за ошибки проверки границ данных в Community Services Multiplexer (StMux.exe) при обработке URL. Удаленный пользователь может с помощью слишком длинного HTTP-запроса, отправленного Sametime-серверу, вызвать переполнение стека и выполнить произвольный код на целевой системе.

**URL производителя:** [www-142.ibm.com/software/sw-lotus/sametime](http://www-142.ibm.com/software/sw-lotus/sametime).

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

Составил Александр Антипов