

## Несколько уязвимостей в IBM Lotus Quickr

**Программа:** IBM Lotus Quickr версии до 8.1.0.1.

**Опасность:** Средняя.

**Описание:** 1. Две уязвимости существуют из-за того, что редактор способен удалить страницы, созданные другим автором, а place manager способен удалить группу place superuser.

2. Уязвимость существует из-за неизвестной ошибки при обработке команды OpenDocument. Удаленный пользователь может с помощью специально сформированного URL аварийно завершить работу сервера.

**URL производителя:** [www-306.ibm.com/software/lotus/products/quickr](http://www-306.ibm.com/software/lotus/products/quickr).

**Решение:** Установите последнюю версию 8.1.0.1 с сайта производителя.

## Несколько уязвимостей при обработке PIM-пакетов в Cisco IOS

**Программа:** Cisco IOS 12.x, Cisco IOS R12.x.

**Опасность:** Средняя.

**Описание:** 1. Уязвимость существует из-за ошибки при обработке пакетов-PIM (Protocol Independent Multicast). Удаленный пользователь может с помощью специально сформированного PIM-пакета вызвать перезагрузку устройства.

2. Уязвимость существует из-за ошибки при обработке пакетов-PIM (Protocol Independent Multicast). Удаленный пользователь может с помощью специально сформированного PIM-пакета аварийно завершить работу устройства. Уязвимости подвержены только маршрутизаторы Cisco 12000 Series (GSR).

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

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

## Уязвимость при обработке SSL-пакетов в Cisco IOS

**Программа:** Cisco IOS 12.4(16)MR, 12.4(16)MR1, 12.4(16)MR2, 12.4(17).

**Опасность:** Средняя.

**Описание:** Уязвимость существует из-за ошибки при обработке SSL-пакетов во время завершения SSL-сессии. Удаленный пользователь может вызвать перезагрузку устройства.

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

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

## Отказ в обслуживании в Cisco IOS Software Firewall

**Программа:** Cisco IOS 12.4(9)T.

**Опасность:** Средняя.

**Описание:** Уязвимость существует из-за ошибки при обработке транзитных HTTP-пакетов при включенном Software Firewall AIC (Application Inspection Control). Удаленный пользователь может с помощью специально сформированных HTTP-пакетов вызвать перезагрузку устройства.

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

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

## Несколько уязвимостей в Serv-U File Server

**Программа:** Serv-U File Server 7.3.0.0, возможно, более ранние версии.

**Опасность:** Средняя.

**Описание:** 1. Уязвимость существует из-за недостаточной проверки входных данных в службе FTP при переименовании файлов. Удаленный пользователь может с помощью символов обхода каталога перезаписать или создать произвольные файлы на системе.

Пример:

```
220 Serv-U FTP Server v7.2 ready...
user test
331 User name okay, need password.
pass test
230 User logged in, proceed.
rnfr any_exist file.ext
350 File or directory exists, ready for destination name.
rnto ..\..\..\boot.ini
250 RNT0 command successful.
```

2. Уязвимость существует из-за ошибки в FTP-команде STOU. Удаленный пользователь может с помощью специально сформированного аргумента команды потребить все доступные процессорные ресурсы.

Пример:

```
220 Serv-U FTP Server v7.2 ready...
user test
331 User name okay, need password.
pass test
230 User logged in, proceed.
stou con:1
quit
221 Goodbye, closing session.
```

**URL производителя:** [www.serv-u.com](http://www.serv-u.com).

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

## Уязвимость при обработке L2TP-пакетов в Cisco IOS

**Программа:** Cisco IOS 12.2 и 12.4.

**Опасность:** Средняя.

**Описание:** Уязвимость существует из-за ошибки в L2TP mgmt-демоде. Удаленный пользователь может с помощью специально сформированного L2TP-пакета вызвать перезагрузку устройства.

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

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

## Отказ в обслуживании в Cisco IOS IPS

**Программа:** Cisco IOS 12.x, Cisco IOS R12.x.

**Опасность:** Средняя.

**Описание:** Уязвимость существует из-за ошибки при обработке определенных IPS-сигнатур, используемых в механизме SERVICE.DNS. Удаленный пользователь может с помощью специально сформированного сетевого трафика аварийно завершить работу устройства.

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

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

Составил Александр Антипов