

## Множественные уязвимости в VMware Server

**Программа:** VMware Server версии до 1.0.7 build 108231.

**Опасность:** Высокая.

**Описание:** 1. Уязвимости существуют из-за неизвестных ошибок в определенных ActiveX-компонентах. Удаленный пользователь может с помощью специально сформированного веб-сайта выполнить произвольный код на целевой системе.

2. Уязвимость существует из-за неизвестной ошибки при обработке запросов в расширении ISAPI. Удаленный пользователь может с помощью специально сформированного запроса вызвать отказ в обслуживании.

3. Уязвимость существует из-за неизвестной ошибки, относящейся к OpenProcess. Локальный пользователь хостовой системы может выполнить произвольный код с повышенными привилегиями на хостовой системе.

4. Уязвимость существует из-за использования уязвимого кода библиотеки freetype. Удаленный пользователь может скомпрометировать целевую систему.

**URL производителя:** [www.vmware.com/products/server](http://www.vmware.com/products/server).

**Решение:** Установите последнюю версию 1.0.7 build 108231 с сайта производителя.

## Множественные уязвимости в xine-lib

**Программа:** xine-lib 1.1.14 и 1.1.15, возможно, более ранние версии.

**Опасность:** Высокая.

**Описание:** 1. Уязвимость существует из-за целочисленного переполнения в функции `open_ra_file()` в файле `src/demuxers/demux_realaudio.c`. Удаленный пользователь может с помощью специально сформированного RealAudio-файла вызвать переполнение динамической памяти и выполнить произвольный код на целевой системе.

2. Уязвимость существует из-за ошибки проверки границ данных в функции `parse_block_group()` в файле `src/demuxers/demux_matroska.c`. Удаленный пользователь может с помощью специально сформированного Matroska-файла вызвать переполнение динамической памяти и выполнить произвольный код на целевой системе.

**URL производителя:** [xinehq.de](http://xinehq.de).

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

## Множественные уязвимости в VMware Fusion

**Программа:** VMware Fusion 1.x.

**Опасность:** Высокая.

**Описание:** 1. Уязвимость существует из-за использования уязвимого кода библиотеки freetype. Удаленный пользователь может скомпрометировать целевую систему.

2. Уязвимость существует из-за использования уязвимой версии библиотеки cairo. Удаленный пользователь может скомпрометировать целевую систему. Уязвимости подвержены только VMware Player 2.x for Linux.

**URL производителя:** [www.vmware.com/products/fusion](http://www.vmware.com/products/fusion).

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

## Множественные уязвимости в VMware ACE

**Программа:** VMware ACE версии до 1.0.7 build 108880 и 2.0.5 build 109488.

**Опасность:** Высокая.

**Описание:** 1. Уязвимости существуют из-за неизвестных ошибок в определенных ActiveX-компонентах. Удаленный пользователь может с помощью специально сформированного веб-сайта выполнить произвольный код на целевой системе.

2. Уязвимость существует из-за неизвестной ошибки, относящейся к OpenProcess. Локальный пользователь хостовой системы может выполнить произвольный код с повышенными привилегиями на хостовой системе. Уязвимости подвержены только VMware ACE 1.x for Windows.

**URL производителя:** [www.vmware.com/products/ace](http://www.vmware.com/products/ace).

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

## Множественные уязвимости в VMware Workstation

**Программа:** VMware Workstation версии до 5.5.8 build 108000 и 6.0.5 build 109488.

**Опасность:** Высокая.

**Описание:** 1. Уязвимости существуют из-за неизвестных ошибок в определенных ActiveX-компонентах. Удаленный пользователь может с помощью специально сформированного веб-сайта выполнить произвольный код на целевой системе.

2. Уязвимость существует из-за неизвестной ошибки, относящейся к OpenProcess. Локальный пользователь хостовой системы может выполнить произвольный код с повышенными привилегиями на хостовой системе.

3. Уязвимость существует из-за использования уязвимого кода библиотеки freetype. Удаленный пользователь может скомпрометировать целевую систему.

4. Уязвимость существует из-за использования уязвимой версии библиотеки cairo. Удаленный пользователь может скомпрометировать целевую систему. Уязвимости подвержена только VMware Workstation 6.x for Linux.

**URL производителя:** [www.vmware.com/download/ws](http://www.vmware.com/download/ws).

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

## Уязвимость в WebSphere Application Server

**Программа:** IBM WebSphere Application Server версии до 6.1.0.19.

**Опасность:** Средняя.

**Описание:** Уязвимость существует из-за неизвестной ошибки в Servlet Engine/Web Container при включенном функционале FileServing. Подробности не раскрываются.

**URL производителя:** [www-306.ibm.com/software/webservers/appserv/was](http://www-306.ibm.com/software/webservers/appserv/was).

**Решение:** Установите исправление Fix Pack 19 (6.1.0.19) с сайта производителя.

Составил Александр Антипов