

Множественные уязвимости в Fedora

Программа: Fedora 8, 9.

Опасность: Средняя.

Описание: 1. Уязвимость существует из-за ошибки проверки границ данных в различных Red Hat Directory Server CGI-приложениях при обработке HTTP-заголовка Accept-Language. Удаленный пользователь может с помощью специально сформированного HTTP-запроса вызвать переполнение буфера и выполнить произвольный код на целевой системе с привилегиями учетной записи root.

2. Уязвимость существует из-за недостаточной обработки данных, содержащих символ «%» в Directory Server Administration Express и Directory Server Gateway (DSGW). 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 недостаточной обработки входных кодированных данных, содержащих символ «%». Удаленный пользователь может с помощью специально сформированного запроса к определенным CGI-приложениям вызвать переполнение динамической памяти и выполнить произвольный код на целевой системе.

URL производителя: fedoraproject.org.

Решение: Установите исправление с сайта производителя.

Отказ в обслуживании в Wireshark

Программа: Wireshark, возможно, более ранние версии.

Опасность: Средняя.

Описание: 1. Различные ошибки обнаружены в `epan/dissectors/packet-ncp2222.inc`. Удаленный пользователь может с помощью специально сформированных NCP-пакетов вызвать заикливание или аварийно завершить работу приложения. Уязвимости подвержены версии с 0.9.7 по 1.0.2.

2. Уязвимость существует из-за ошибки при декомпрессии zlib-сжатых данных. Удаленный пользователь может с помощью специально сформированных пакетов вызвать отказ в обслуживании приложения. Уязвимости подвержены версии с 0.10.14 по 1.0.2.

URL производителя: www.wireshark.org.

Решение: Установите последнюю версию 1.0.3 с сайта производителя.

Уязвимость форматной строки в HP TCP/IP Services for OpenVMS

Программа: HP TCP/IP Services for OpenVMS 5.x.

Опасность: Средняя.

Описание: Уязвимость существует из-за ошибки форматной строки в finger-клиенте. Удаленный пользователь может с помощью специально сформированных .plan или .project-файлов, расположенных в домашней директории пользователя, выполнить произвольный код на целевой системе. Для успешной эксплуатации уязвимости злоумышленник должен обманом заставить пользователя подключиться к злонамеренному finger-серверу.

URL производителя: h71000.www7.hp.com/network/tcpip.html.

Решение: В настоящее время способов устранения уязвимости не существует.

Множественные уязвимости в VMware Player

Программа: VMware Player версии до 1.0.8 build 108000 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 Player 1.x for Linux.

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 подвержены только VMware Player 2.x for Linux.

URL производителя: www.vmware.com/products/player.

Решение: Установите последнюю версию с сайта производителя.

Выполнение произвольного кода в Dns2tcp

Программа: Dns2tcp версии до 0.4.1.

Опасность: Высокая.

Описание: Уязвимость существует из-за знаковой ошибки при обработке запросов или ответов в функции `dns_simple_decode()` в файле `common/dns.c` и в функции `dns_decode()` в файле `server/dns_decode.c`. Удаленный пользователь может с помощью специально сформированного запроса или ответа вызвать повреждение памяти и вызвать отказ в обслуживании или выполнить произвольный код на целевой системе.

URL производителя: www.hsc.fr/ressources/outils/dns2tcp/index.html.en.

Решение: Установите последнюю версию 0.4.1 с сайта производителя.

Отравление DNS-кэша в Ingate Firewall и SIParator

Программа: Ingate Firewall версии до 4.6.4; Ingate SIParator версии до 4.6.4.

Опасность: Средняя.

Описание: Уязвимость существует из-за того, что Ingate Firewall и SIParator используют предсказуемый номер порта при включенном NAT. Удаленный пользователь может отправить кэш DNS-сервера и произвести спуфинг-атаку.

URL производителя: www.ingate.com.

Решение: Установите последнюю версию 4.6.4 с сайта производителя.

Составил Александр Антипов