

## Множественные уязвимости в IBM AIX

**Программа:** IBM AIX 5.2, 5.3 и 6.1.

**Опасность:** Низкая.

**Описание:** 1. Уязвимость существует из-за того, что 64-битный процесс после перезагрузки посредством checkpoint и функционала перезапуска получает доступ для чтения и записи к некоторым участкам памяти ядра. Локальный пользователь может выполнить произвольный код на целевой системе.

2. Уязвимость существует из-за неизвестной ошибки, которая позволяет аварийно завершить работу удаленных узлов параллельной группы тома, когда один узел уменьшает размер файловой системы JFS2 на параллельной группе тома.

3. Уязвимость существует из-за того, что файловая система rpgs некорректно накладывает ограничения на доступ к директории, когда привилегии на директорию являются более строгими, чем привилегии на выполняемый файл в директории.

4. Уязвимость существует из-за ошибки в системных вызовах WPAR. Локальный пользователь может вызвать отказ в обслуживании системы.

5. Уязвимость существует из-за неизвестной ошибки, которая позволяет пользователю с привилегиями на запуск ProbeVue получить доступ на чтение произвольных участков памяти ядра.

6. Уязвимость существует из-за неизвестной ошибки при обработке переменных окружения в командах atmstat, entstat, fddistat, hdlcstat и tokstat из семьи nddstat и в команде lsmcode. Локальный пользователь может выполнить произвольный код на системе с привилегиями учетной записи root.

**URL производителя:** [www-1.ibm.com/servers/eserver/pseries/software](http://www-1.ibm.com/servers/eserver/pseries/software).

**Решение:** Для решения проблемы следуйте инструкциям производителя.

## Отказ в обслуживании в Sun Solaris

**Программа:** Sun Solaris 10.

**Опасность:** Низкая.

**Описание:** Уязвимость существует из-за неизвестной ошибки в модуле ядра ipsec(7P). Локальный пользователь может вызвать панику ядра системы. Для успешной эксплуатации уязвимости на системе должен использоваться IPsec, и хотя бы одно приложение должно слушать на PF\_KEY сокете.

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

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

## Отказ в обслуживании в Sun Solaris

**Программа:** Sun Solaris 10.

**Опасность:** Низкая.

**Описание:** Уязвимость существует из-за ошибки в rpc.metad. Удаленный пользователь может с помощью специально сформированного RPC-запроса аварийно завершить работу демона.

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

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

## Отказ в обслуживании в ZABBIX

**Программа:** ZABBIX 1.4.4, возможно, более ранние версии.

**Опасность:** Низкая.

**Описание:** Уязвимость существует из-за некорректной реализации команды `vfs.file.cksum` в `zabbix_agentd`. Удаленный пользователь может с помощью большого количества команд `vfs.file.cksum`, отправленных на порт 10050/TCP и содержащих `«/dev/urandom»` в качестве параметра, заставить обработку валидных запросов. Для успешной эксплуатации уязвимости, команды должны быть отправлены с доверенного хоста.

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

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

## Переполнение буфера в user-ppp

**Программа:** user-ppp.

**Опасность:** Низкая.

**Описание:** Уязвимость существует из-за ошибки проверки границ данных в функции `command_Expand_Interpret()` в файле `command.c`. Локальный пользователь может с помощью строки, содержащей определенные символы (например, `'~'`), вызвать переполнение стека и повысить свои привилегии на системе. Для успешной эксплуатации уязвимости атакующий должен иметь привилегии группы `network`.

**URL производителя:** [www.awfulhak.org/ppp.html](http://www.awfulhak.org/ppp.html).

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

## Переполнение буфера в IBM AIX

**Программа:** IBM AIX 5.2 и 5.3.

**Опасность:** Низкая.

**Описание:** Уязвимость существует из-за ошибки проверки границ данных в команде `reboot`. Локальный пользователь, член группы `shutdown`, может вызвать переполнение стека и выполнить произвольный код на целевой системе с привилегиями учетной записи `root`.

**URL производителя:** [www-1.ibm.com/servers/eserver/pseries/software](http://www-1.ibm.com/servers/eserver/pseries/software).

**Решение:** Для решения проблемы следуйте инструкциям производителя.

## Внедрение FTP-команд в Microsoft Internet Explorer

**Программа:** Microsoft Internet Explorer 5.01, Microsoft Internet Explorer 6.x.

**Опасность:** Низкая.

**Описание:** Уязвимость существует из-за ошибки проверки входных данных при обработке FTP URI. Удаленный пользователь может с помощью специально сформированного FTP URI, содержащего CRLF-последовательности и слеша, внедрить и выполнить произвольные FTP-команды в контексте FTP-сессии пользователя.

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

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

Составил Александр Антипов