

## Множественные уязвимости в MailEnable

**Программа:** MailEnable Enterprise Edition 3.13, возможно, более ранние версии; MailEnable Professional 3.13, возможно, более ранние версии.

**Опасность:** Средняя.

**Описание:** 1. Уязвимость существует из-за ошибки проверки границ данных в службе IMAP (MEIMAPS.EXE) при обработке аргументов, передаваемых командам FETCH, EXAMINE и UNSUBSCRIBE. Удаленный авторизованный пользователь может с помощью слишком длинного аргумента вызвать переполнение буфера и выполнить произвольный код на целевой системе.

2. Уязвимость существует из-за ошибки в службе IMAP при обработке команд SEARCH и APPEND. Удаленный пользователь может с помощью специально сформированной команды аварийно завершить работу службы.

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

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

## Множественные уязвимости в IBM WebSphere Application Server

**Программа:** IBM WebSphere Application Server 6.1.x.

**Опасность:** Средняя.

**Описание:** 1. Уязвимость существует из-за неизвестной ошибки в wsadmin в компоненте Administrative Scripting Tools. Подробности уязвимости не сообщаются.

2. Уязвимость существует из-за неизвестной ошибки в утилите PropFilePasswordEncoder. Подробности уязвимости не сообщаются.

3. Уязвимость существует из-за того, что некоторые потенциально важные данные хранятся в открытом виде в файлах http\_plugin.log (компонент Plug-in) и startserver.log (компонент System Management/Repository).

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

**Решение:** Установите исправление Fix Pack 15 (6.1.0.15) с сайта производителя.

## Множественные уязвимости в IBM Informix Dynamic Server

**Программа:** IBM Informix Dynamic Server 7.x, 9.x, 10.x, 11.x

**Опасность:** Средняя.

**Описание:** 1. Уязвимость существует из-за неизвестной ошибки при обработке запросов на подключения.

2. Уязвимость существует из-за ошибки проверки границ данных в oinit.exe при обработке переменной DBPATH во время аутентификации. Удаленный пользователь может отправить слишком длинную переменную DBPATH на порт приложения 1526/TCP и вызвать переполнение буфера.

3. Уязвимость существует из-за ошибки проверки границ данных в oinit.exe при обработке паролей во время аутентификации. Удаленный пользователь может с помощью слишком длинного пароля, отправленного на порт 1526/TCP, вызвать переполнение стека.

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

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

## Отказ в обслуживании в MailEnable

**Программа:** MailEnable Enterprise Edition 1.x, MailEnable Enterprise Edition 2.x, MailEnable Enterprise Edition 3.x, MailEnable Professional 1.x, MailEnable Professional 2.x, MailEnable Professional 3.x, MailEnable Standard 1.x.

**Опасность:** Средняя.

**Описание:** Уязвимость существует из-за неизвестной ошибки в службе SMTP при обработке команд EXPN и VRFY. Удаленный пользователь может с помощью специально сформированной команды аварийно завершить работу службы.

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

**Решение:** Установите исправление ME-10039 с сайта производителя.

## Уязвимость форматной строки в McAfee ePolicy Orchestrator

**Программа:** McAfee ePolicy Orchestrator 4.0.0 (build 1015), возможно, более ранние версии.

**Опасность:** Средняя.

**Описание:** Уязвимость существует из-за ошибки форматной строки в McAfee Framework Service (FrameworkService.exe версия 3.6.0.569). Удаленный пользователь может отправить специально сформированный пакет, содержащий символы форматной строки, на порт 8082/UDP и выполнить произвольный код на целевой системе.

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

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

## Раскрытие данных в Ruby

**Программа:** Ruby 1.9.0-1 и более ранние версии, Ruby версии до 1.8.5-p115 и 1.8.6-p114.

**Опасность:** Средняя.

**Описание:** 1. Уязвимость существует из-за недостаточной обработки URL в приложениях, использующих «WEBrick::HTTPServlet::FileHandler» или «WEBrick::HTTPServer.new» с опцией «:DocumentRoot». Удаленный пользователь может с помощью специально сформированного URL, содержащего символы обхода каталога (например, «..%5c..%5c»), просмотреть содержимое произвольных файлов на системе. Для успешной эксплуатации уязвимости приложение должно работать на системе, воспринимающей обратный слеш как разделитель пути (например, Windows).

2. Уязвимость существует из-за ошибки в классе «WEBrick::HTTPServlet::FileHandler» и в методе «WEBrick::HTTPServer.new» при обработке опции «:NondisclosureName». Удаленный пользователь может просмотреть содержимое произвольных файлов на системе, если имя файла соответствует условию, определенному в опции «:NondisclosureName».

**URL производителя:** [www.ruby-lang.org/en](http://www.ruby-lang.org/en).

**Решение:** Установите последнюю версию 1.8.5-p115 или 1.8.6-p114 или исправление для версии 1.9.0-1 с сайта производителя.

Составил Александр Антипов