Найдена критическая уязвимость в браузере Opera

Автор: newsland.ru
15.03.2010 18:59

Компания Secunia выявила серьезную уязвимость в браузере Opera. Критический баг, вызывающий переполнение буфера, позволяет хакеру получить удаленный доступ к машине жертвы и осуществить на ней выполнение произвольного кода.

Подобного рода неприятности с этим браузером довольно редки, последний раз серьезная уязвимость в Opera была выявлена осенью 2008 года.

На данный момент патч, закрывающий описанную выше брешь, еще не выпущен. Пользователям советуют не посещать подозрительные сайты или отказаться от использования Opera до момента выхода соответствующего обновления.

По словам эксперта Secunia Марцина Рессела, уязвимость проявляется вследствие ошибки при обработке специальным образом составленного HTTP-заголовка Content-Length. Эту недоработку можно использовать для переполнения буфера в куче путем установки чрезмерно большого значения 64-битного заголовка.

В данный момент достоверно известно о том, что данной уязвимости подвержена версия Opera за номером 10.50, однако по мнению ряда специалистов, баг может проявляться и в более ранних сборках этого веб-обозревателя.

Эксперты также предупреждают о том, что действующий эксплоит, использующий данную уязвимость, легко доступен в Сети, однако пока что нет данных об использовании уязвимости злоумышленниками.

Источник: newsland.ru