Автор: Administrator
18.03.2016 17:59

{jcomments on}

В сентябре прошлого года Microsoft сообщила о намерении прекратить поддержку потокового шифра RC4 в своих браузерах, и теперь компания готовит обновление, деактивирующее его в Internet Explorer 11 и Edge. Нововведение вступит в силу 12 апреля нынешнего года с выходом кумулятивного патча.

В настоящее время в Internet Explorer 11 и Edge шифр RC4 используется только в случае отката от TLS 1.2 или TLS 1.1 до TLS 1.0. Как сообщают в Microsoft, откат до TLS 1.0 с применением RC4 представляет собой малозначительную проблему. Тем не менее, данная ошибка неотличима от атаки «человек посередине» и поэтому должна быть полностью деактивирована. Отключение RC4 никак не скажется на взаимодействии пользователей с большинством web-сервисов, поскольку многие из них уже отказались от данного шифра.

Microsoft советовала клиентам отказаться от использования разработанного в 1987 году RC4 еще три года назад. С выходом последних обновлений шифр деактивирован в браузерах Google Chrome, Mozilla Firefox и Opera.

Источник: www.securitylab.ru