В браузере Tor исправлены две DoS-уязвимости

Разработчики браузера Tor выпустили новые корректирующие версии (0.3.5.10, 0.4.1.9, 0.4.2.7, 0.4.3.3-alpha), исправляющие две уязвимости.

Первая уязвимость (CVE-2020-10592) может быть проэксплуатирована любым злоумышленником для вызова отказа в обслуживании узлов. Атака также может быть осуществлена со стороны серверов каталогов Tor для атаки на подключенные клиенты и скрытые сервисы. Преступник способен своими действиями вызвать большую нагрузку на CPU и нарушить нормальною работу на несколько секунд или минут, а также многократно повторять данную атаку. Проблема затрагивает все версии браузера, начиная с выпуска 0.2.1.5-alpha.

Вторая проблема (CVE-2020-10593) представляет собой удаленно эксплуатируемую утечку памяти, возникающую при двойном согласовании добавочных ячеек для одной и той же цепочки.

В версии браузера Tor 9.0.6 остается неисправленной уязвимость в дополнении NoScript, позволяющая осуществить запуск JavaScript-кода в режиме защиты "Safest". Проблему пытались устранить в NoScript 11.0.17, но предложенное исправление не смогло полностью решить проблему. В Tor включено автоматическое обновление NoScript, поэтому пользователи получат исправление сразу после его выхода.

Источник: https://www.securitylab.ru/news/506019.php