Месяц поиска уязвимостей в Яндексе — 2015

В интернете каждый день появляются новые угрозы. Единственный способ защитить пользователей своего продукта — постоянно поддерживать безопасность на высоком уровне. Команда Яндекс.Браузера предлагает вам внести свой вклад в эту задачу и объявляет конкурс «Месяц поиска уязвимостей в Яндексе — 2015».

До 20 ноября 2015 года любой желающий может попытаться найти уязвимость в Браузере и сообщить о ней Яндексу. Самых активных участников ждёт денежное вознаграждение.

Что такое уязвимость

Уязвимость — технический недостаток, с помощью которого можно нарушить целостность или конфиденциальность пользовательской информации, а также изменить права доступа к ней. Уязвимости нужно искать только в стабильной версии Яндекс.Браузера не ниже 15.10 (не в бета-версии) для операционных систем Windows и OS X. Уязвимости, доступные в публичных источниках информации (в том числе в интернете), на конкурс не принимаются.

Что нужно искать

Уязвимости, которые учитываются в конкурсе, различаются по степени критичности. Таких степеней пять: от P1 (наивысшая степень) до P5 (наименьшая).

- Возможность удалённого выполнения кода (remote code execution) через Use-After-Free, Integer Overflow, Stack/Heap Based Overflow, Memory Corruption и т.д. (P1)
- Возможность обхода защиты в общественных сетях Wi-Fi (механизм Protect), а именно создания незащищённого подключения в открытой сети Wi-Fi либо перехвата/модификации HTTP-трафика.
- Возможность обхода защиты паролей (механизм Protect), а именно получения пароля пользователя, совпадающего с паролем от Яндекса, в обход предупреждения о вводе пароля от Яндекса на другом сайте. (Принимаются только методы обхода защиты при вводе паролей через стандартные веб-формы HTML вида **<input type=password>**.) (P5)
- Возможность обхода защиты паролей (механизм Protect) путём подбора пароля от Яндекса. (P1)
- Возможность обхода Same Origin Policy (SOP), а именно выполнения Universal XSS (UXSS), обхода SOP через Cache-Timing, а также Browser-API уязвимость. (P2)
- Возможность обхода Content Security Policy (CSP) за исключением обхода CSP через расширения браузера или подмену HTTP-заголовков. (P3)
- Ошибки в реализации SSL\TLS, проверке сертификатов, проведении SSL-Strip с сохранением статуса защищённого соединения у ресурса. (P3)
- Возможность запускать старые версии плагинов без подтверждения пользователем (click-to-play bypass). (P4)
- Удалённый отказ в обслуживании (Remote DoS) через JS или HTML. (P5)

Призы
1 место — 500 000 рублей
2 место — 300 000 рублей
3 место — 150 000 рублей

Как сообщать об уязвимостях
Отправлять находки на конкурс нужно через специальную форму — https://yandex.ru/bugbounty/report/

Сроки и результаты

Сообщения принимаются с 26 октября 2015 года по 20 ноября 2015 года, до 23:59 по московскому времени.

Конкурсная комиссия оценит результаты участников в баллах и определит трёх победителей, приславших самые опасные и интересные уязвимости.

Победители будут объявлены 26 ноября 2015 года на конференции ZeroNights — 2015 и в блоге Яндекс.Браузера. Призёры, которые будут на конференции, также получат сувениры Яндекса.

Ограничения и политика ответственного разглашения

Просьба не рассказывать о найденных уязвимостях в течение 30 дней после отправки сообщения на конкурс. Также, пожалуйста, не размещайте код обнаруженной уязвимости на публичных ресурсах, чтобы информация не попала к третьим лицам. Для тестирования и демонстрации уязвимостей можно использовать только свою учётную запись. Взламывать чужие ни в коем случае нельзя. Это обязательные правила. Если вы их нарушите, то не сможете участвовать в конкурсе.

Положение конкурса доступно по адресу
download.cdn.yandex.net/browser/ZN/legal.pdf