Рекомендации Mozilla Foundation по безопасности 2019-21

Уязвимости безопасности исправлены в Firefox 68

- Объявлено 9 июля 2019 г.
- Влияние критический
- Продукты Fire Fox
- Исправлено в Фаерфокс 68

CVE-2019-9811: выход из песочницы посредством установки вредоносного языкового пакета.

Репортер Никлас Баумстарк Влияние высокий Описание В рамках своей победившей работы на Pwn2Own Никлас Баумстарк продемонстрировал выход из «песочницы», установив вредоносный языковой пакет, а затем открыв функцию браузера, которая использовала скомпрометированный перевод.

Рекомендации Ошибка 1538007 Ошибка 1539598 Ошибка 1539759 Ошибка 1523741 Ошибка 1563327

CVE-2019-11711: внедрение скриптов в домен посредством повторного использования внутреннего окна.

Репортер Борис Збарский Влияние высокий Описание При повторном использовании внутреннего окна не учитывается использование document.domainдля защиты от перекрестного происхождения. Если страницы в разных поддоменах когда-либо совместно используют document.domain, то любая страница может злоупотребить этим, чтобы внедрить скрипт в произвольные страницы в другом поддомене, даже в те, которые не использовали document.domainдля ослабления безопасности своего происхождения.

Рекомендации Ошибка 1552541

CVE-2019-11712: POST-запросы между источниками можно выполнять с помощью подключаемых модулей NPAPI, следуя 308-м перенаправлениям.

Репортер Грегори Смайли из Security Compass Влияние высокий Описание Запросы POST, сделанные подключаемыми модулями NPAPI, такими как Flash, которые получают ответ

перенаправления со статусом 308, могут обойти требования CORS. Это может позволить злоумышленнику выполнить атаку с подделкой межсайтовых запросов (CSRF).

Рекомендации Ошибка 1543804

CVE-2019-11713: использование после освобождения с кэшированным потоком HTTP/2.

Репортер Ханно Бёк Влияние высокий Описание Уязвимость использования после освобождения может возникнуть в HTTP/2, когда кэшированный поток HTTP/2 закрывается, пока он еще используется, что приводит к потенциально опасному сбою.

Рекомендации Ошибка 1528481

CVE-2019-11714: NeckoChild может вызвать сбой при доступе вне основного потока.

Репортер Ханно Бёк Влияние умеренный Описание Necko может получить доступ к дочернему элементу в неправильном потоке во время UDP-соединений, что в некоторых случаях приводит к потенциально опасному сбою.

Рекомендации Ошибка 1542593

CVE-2019-11729: пустые или неправильно сформированные открытые ключи p256-ECDH могут вызвать ошибку сегментации.

Репортер Йонас Аллманн Влияние умеренный Описание Пустые или неправильно сформированные открытые ключи p256-ECDH могут вызвать ошибку сегментации из-за неправильной очистки значений перед копированием в память и использованием.

Рекомендации Ошибка 1515342

CVE-2019-11715: ошибка синтаксического анализа HTML может способствовать XSS контента.

Репортер Линус Сяруд Влияние умеренный Описание Из-за ошибки при синтаксическом анализе содержимого страницы правильно обработанный пользовательский ввод может быть неправильно истолкован и при определенных обстоятельствах приведет к возникновению угроз XSS на веб-сайтах.

Рекомендации Ошибка 1555523

CVE-2019-11716: globalThis не перечисляется до тех пор, пока к нему не будет получен доступ.

Репортер Крис Хакинг Влияние умеренный Описание До тех пор, пока к нему не будет явный доступ со стороны сценария, window.globalThison не является перечислимым и, как следствие, не виден для такого кода, как Object.getOwnPropertyNames(window). Сайты, развертывающие песочницу, зависящую от перечисления и блокировки доступа к объекту окна, могут пропустить это, что позволяет обходить их песочницы.

Рекомендации Ошибка 1552632

CVE-2019-11717: Символ вставки неправильно экранирован в исходном коде.

Репортер Тайсон Смит Влияние умеренный Описание Существует уязвимость, при которой символ каретки («^») неправильно экранируется при создании некоторых URI, поскольку он используется в качестве разделителя, что позволяет подделать атрибуты происхождения.

Рекомендации Ошибка 1548306

CVE-2019-11718: поток активности записывает несанкционированный контент во внутренний HTML.

Репортер Марк Баннер Влияние умеренный Описание Лента активности может отображать контент, отправленный с веб-сайта службы фрагментов. Этот контент записывается на innerHTMLстраницу ленты активности без очистки, что обеспечивает потенциальный доступ к другой информации, доступной для ленты активности, такой как история просмотров, если служба Snipper была скомпрометирована.

Рекомендации Ошибка 1408349

CVE-2019-11719: Чтение за пределами границ при импорте закрытого ключа Curve25519.

Репортер Генри Корриган-Гиббс Влияние умеренный Описание При импорте закрытого ключа Curve25519 в формате PKCS#8 с ведущими байтами 0x00 можно инициировать чтение за пределами границ в библиотеке Network Security Services (NSS). Это может привести к раскрытию информации.

Рекомендации Ошибка 1540541

CVE-2019-11720: XSS-уязвимость кодировки символов.

Репортер Ракеш Мане Влияние умеренный Описание Некоторые символы Юникода неправильно обрабатываются как пробелы во время анализа веб-контента вместо того, чтобы вызывать ошибки анализа. Это позволяет затем обрабатывать вредоносный код, избегая фильтрации межсайтового скриптинга (XSS).

Рекомендации Ошибка 1556230

CVE-2019-11721: Подмена домена с помощью латинского символа «kra» в Юникоде.

Репортер Анонимный Влияние умеренный Описание Латинский символ «kra» в Юникоде можно использовать для подмены стандартного символа «k» в адресной строке. Это позволяет проводить атаки по подмене домена, поскольку они не отображаются в виде текста в формате Punycode, что приводит к путанице пользователей.

Рекомендации Ошибка 1256009

CVE-2019-11730: политика одинакового происхождения рассматривает все файлы в каталоге как имеющие одинаковое происхождение.

Репортер Луиджи Губелло Влияние умеренный Описание Существует уязвимость: если пользователь открывает локально сохраненный HTML-файл, этот файл может использовать file:URI для доступа к другим файлам в том же каталоге или подкаталогах, если имена известны или угаданы. Затем API Fetch можно использовать для чтения содержимого любых файлов, хранящихся в этих каталогах, и их можно загрузить на сервер. Луиджи Губелло продемонстрировал, что в сочетании с популярным приложением для обмена сообщениями Android, если пользователю отправлено вредоносное HTML-вложение и он открыл это вложение в Firefox, благодаря предсказуемому шаблону этого приложения для локально сохраненных имен файлов можно прочитать вложения. потерпевшая получила от других корреспондентов.

Рекомендации Ошибка 1558299

CVE-2019-11723: утечка файлов cookie во время загрузки надстройки через границы частного просмотра.

Репортер Андреас Вагнер Влияние низкий Описание Во время установки надстроек существует уязвимость, из-за которой при первоначальной выборке игнорировались атрибуты

происхождения контекста просмотра. Это может привести к утечке файлов cookie в режиме приватного просмотра или в разных «контейнерах» для людей, использующих веб-расширение Firefox для нескольких учетных записей-контейнеров.

Рекомендации Ошибка 1528335

CVE-2019-11724: устаревший сайт input.mozilla.org имеет разрешения на удаленное устранение неполадок.

Репортер Фредерик Браун Влияние низкий Описание Разрешения для приложений предоставляют дополнительные разрешения на удаленное устранение неполадок для сайта input.mozilla.org, который больше не используется и теперь перенаправляется на другой сайт. Это дополнительное разрешение не является необходимым и является потенциальным вектором вредоносных атак.

Рекомендации Ошибка 1512511

CVE-2019-11725: ресурсы Websocket обходят защиту безопасного просмотра.

Репортер Андрей Влияние низкий Описание Когда пользователь переходит на сайт, отмеченный API безопасного просмотра как небезопасный, отображаются предупреждающие сообщения и навигация прерывается, но ресурсы с того же сайта, загруженные через веб-сокеты, не блокируются, что приводит к загрузке небезопасных ресурсов и обходу защиты безопасного просмотра.

Рекомендации Ошибка 1483510

CVE-2019-11727: подписи PKCS#1 v1.5 можно использовать для TLS 1.3.

Репортер Юбер Карио Влияние низкий Описание Существует уязвимость, позволяющая заставить службы сетевой безопасности (NSS) подписывать CertificateVerifyподписи PKCS#1 v1.5, если только они объявлены сервером в CertificateRequestTLS 1.3. Подписи PKCS#1 v1.5 не следует использовать для сообщений TLS 1.3.

Рекомендации Ошибка 1552208

CVE-2019-11728: сканирование портов через заголовок Alt-Svc.

Репортер Тришита Тивари, Ари Трахтенберг Влияние низкий Описание Заголовок HTTP

Alternative Services ( ) Alt-Svcможет использоваться вредоносным сайтом для сканирования всех TCP-портов любого хоста, доступных пользователю при загрузке веб-контента.

Рекомендации Ошибка 1552993

CVE-2019-11710: исправлены ошибки безопасности памяти в Firefox 68.

Репортер Разработчики и сообщество Mozilla Влияние критический Описание Разработчики и члены сообщества Mozilla Андре Баргулл, Кристиан Холлер, Наталья Чореги, Рауль Гурзау, Даниэль Варга, Джон Копперд, Марсия Ноус, Гэри Квонг, Рэнделл Джесуп, Дэвид Болтер, Джефф Гилберт и Дейан Стефан сообщили об ошибках безопасности памяти, присутствующих в Firefox 67. Некоторые из этих ошибок свидетельствовали о повреждении памяти, и мы предполагаем, что при достаточном усилии некоторые из них можно будет использовать для запуска произвольного кода.

Рекомендации В Firefox 68 исправлены ошибки безопасности памяти

CVE-2019-11709: исправлены ошибки безопасности памяти в Firefox 68 и Firefox ESR 60.8.

Репортер Разработчики и сообщество Mozilla Влияние критический Описание Разработчики Mozilla и члены сообщества Андреа Павел, Кристиан Холлер, Хонза Бамбас, Джейсон Кратцер и Джефф Гилберт сообщили об ошибках безопасности памяти, присутствующих в Firefox 67 и Firefox ESR 60.7. Некоторые из этих ошибок свидетельствовали о повреждении памяти, и мы предполагаем, что при достаточном усилии некоторые из них можно будет использовать для запуска произвольного кода.

Рекомендации Исправлены ошибки безопасности памяти в Firefox 68 и Firefox ESR 60.8.