В браузере Edge разрешены сертификаты, подписанные с помощью SHA-1

Автор: Administrator
02.09.2020 08:53

{jcomments on}

Компания Microsoft опубликовала новый базовый план безопасности для браузера Microsoft Edge, где одно из новых правил озаглавлено «Разрешить сертификаты, подписанные с использованием SHA-1, когда они выдаются локальными якорями доверия».

Национальный институт стандартов и технологий США отказался от использования SHA-1 в 2011 году, а Microsoft удалила его из своих браузеров Internet Explorer и Edge в 2017 году. Данное решение было принято в связи с тем, что алгоритм хеширования был подвержен коллизионным атакам, которые позволяли создавать реплики.

«Microsoft Edge по умолчанию запрещает сертификаты, подписанные с использованием SHA-1, и базовый уровень безопасности обеспечивает это, чтобы предприятия понимали, что разрешение цепочек SHA-1 не является безопасной конфигурацией. Если вам необходимо использовать цепочку SHA-1 для совместимости с существующими приложениями, зависящими от нее, вам необходимо как можно скорее отказаться от подобной в целях безопасности вашей организации», — пояснили представители компании.

В версии 92 Microsoft Edge, запланированной на середину 2021 года, этот параметр будет удален, и после не будет поддерживаемого механизма, разрешающего SHA-1, даже для сертификатов, выпущенных частными центрами сертификации.

Также была добавлена политика под названием «Определить список протоколов, которые могут запускать внешнее приложение из перечисленных источников без запроса пользователя», позволяющая пользователям всегда разрешать браузерам запускать локальные приложения.

Источник: www.securitylab.ru

(function(w, d, n) { w[n] = w[n] || []; w[n].push({ section_id: 263974, place: "advertur_263974", width: 300, height: 250 }); })(window, document, "advertur_sections");