https://xakep.ru/2017/11/06/estonian-id-roca/

7.11.2017

Власти Эстонии отозвали сертификаты 760 000 ID-карт из-за уязвимости ROCA

Мария Нефёдова

1 неделя назад

48 сек на чтение

4

0

6563

Мобильная версия статьи

В середине октября 2017 года сводная группа специалистов, в которую вошли представители чешского университета Масариков, итальянского университета Ка' Фоскари и компании Enigma Bridge, сообщила о криптографической проблеме в TPM компании Infineon Technologies, выпущенных после 2012 года.

Trusted platform module (TPM) используются в бессчетном количестве устройств и гаджетов для генерации RSA-ключей для VPN, шифрования дисков, доступа к обычным аккаунтам, работы с сертификатами и так далее.

По сути, обнаруженный исследователями баг ослабляет криптографию, из-за чего надежность RSA-ключей оказывается под большим вопросом. Уязвимость затронула TPM на базе спецификаций TCG 1.2 и 2.0.

Еще в октябре было известно, что проблема коснулась множества устройств, включая различные девайсы HP, Acer, Fujitsu, Lenovo, LG, «Хромбуки», некоторые токены Yubikey 4, а также выпущенные в Эстонии идентификационные карты, оснащенные специальным чипом и позволяющие использовать криптографические подписи для некоторых операций.

Так как обнаружившие баг исследователи постарались связаться со всеми пострадавшими производителями заблаговременно, это коснулось и швейцарской компании Gemalto AG, которая ранее приобрела фирму Trub AG, разработавшую и поставляющую Эстонии идентификационные карты для граждан. Как показало проведенное эстонскими властями расследование, уязвимости подвержены все ID, выпущенные в период с 14 октября 2014 года по 26 октября 2017 года. В итоге еще в сентябре 2017 года власти страны начали уведомлять владельцев ID и проблеме и необходимости обновления удостоверений личности.

В итоге на прошлой неделе правительство Эстонии поддержало предложение Департамента полиции и погранохраны и Департамента государственных информационных систем, которые предложили остановить действие сертификатов ID-карт из группы риска 24:00 часов 3 ноября 2017 года. Сообщается, что все карты продолжат действовать в качестве удостоверения личности, но их невозможно будет использовать, к примеру, для покупки лекарств по электронным рецептам, работы с налогами, и для осуществления других операций, в которых задействуется криптографический ключ.

«Функционирование электронного государства основывается на доверии, и государство не может допустить воровство личности у владельцев эстонских ID-карт. Согласно имеющейся на данный момент информации, подобных краж не совершалось, однако оценка риска, которую производят полиция и Департамент государственных инфосистем, показывает, что опасность стала вполне реальной», — заявил премьер-министр Юри Ратас.

Теперь карты с закрытыми сертификатами, которых насчитывается порядка 760 000, необходимо обновить в представительствах Департамента полиции и погранохраны или в режиме онлайн. Власти сообщают, что обновить сертификаты дистанционно и в приоритетном порядке смогут только те люди, которые особенно активно используют ID-карты в своей работе. Таких людей насчитывается примерно 35 000, и обновление сертификатов для них уже стартовало 3-5 ноября. Это врачи, те, кто работает в системе права, а также люди, работающие с актами гражданского состояния.

Для обычных граждан обновление сертификатов началось сегодня, 6 ноября 2017 года, и оно продлится до 31 марта 2018 года. После 1 апреля 2017 года, по соображениям безопасности, необновленные сертификаты будут аннулированы. Сообщается, что к концу прошлой недели документы обновили только 20 000 человек.