Программа защиты личных данных TrueCrypt подверглась проверке на критические ошибки

Кирилл Алексеев

https://te-st.org/2014/04/29/the-audit-program-truecrypt/

Статья обновлена 20 декабря 2024

В 2013 году сообщество пользователей инициировало проведение независимого аудита популярной программы для шифрования TrueCrypt. 14 апреля 2014 года первый этап аудита был завершен, и теперь его результаты доступны всем желающим. Серьезных ошибок в работе программы обнаружено не было, однако качество кода аудиторы назвали не очень высоким.

TrueCrypt — одна из самых популярных криптографических программ, согласно статистике, на официальном сайте ее скачали порядка 30 миллионов раз. Несмотря на долгую 10-летнюю историю программы, за все время не проводилось ни одного независимого аудита ее кода. У TrueCrypt нет официального репозитория на GitHub и ясной понятной лицензии. Недавние заявления Эдварда Сноудена о прослушке Интернета Агентством национальной безопасности США вызвали еще больше вопросов к защищенности TrueCrypt.

Пользователи решили сами спонсировать проведение проверки. Сбор средств инициировал программист и специалист по биотехнологиям Кеннет Уайт и профессор Университета Джона Хопкинса Мэтью Грин. Краудфандинговая кампания проводилась на двух площадках — FindFill

и IndieGoGo, собранных 60 тысяч долларов должно хватить не только на проведение аудита, но и на создание публичного репозитория кода, подготовку лицензии. Инициативу поддержала команда разработчиков TrueCrypt.

14 апреля 2014 года первый этап аудита был завершен. В ходе проверки было обнаружено 11 ошибок кода: 4 — средней степени, 4 — низкой и 3 не представляющих никакой угрозы. Критических ошибок обнаружено не было. Полные данные доступны в 32-страничном отчете PDF, в котором для большей наглядности представлена диаграмма, ранжирующая ошибки кода по степени угрозы и легкости эксплуатации.

Несмотря на отсутствие рисков безопасности TrueCrypt, аудиторы отметили не очень высокое качество кода: использование устаревших функций, отсутствие единообразия в типах переменных, недостаток комментариев и др.

Скачать отчет с результатами первого этапа аудита программы TrueCrypt.