ОБНАРУЖЕН СПОСОБ ВОССТАНОВИТЬ КЛЮЧИ ECDSA

Исследователи из университета им. Масарика в Брно (Чехия) опубликовали PoC-код и подробности о нескольких уязвимостях, получивших название Minerva, в различных реализациях алгоритма создания цифровой подписи ECDSA/EdDSA. Их эксплуатация позволяет злоумышленнику восстановить значение закрытого ключа на основе анализа утечек сведений об отдельных битах, всплывающих при применении методов анализа по сторонним каналам.

Данный метод атаки затрагивает проекты OpenJDK/OracleJDK (CVE-2019-2894) и библиотеку Libgcrypt (CVE-2019-13627), применяемую в GnuPG, а также MatrixSSL, Crypto++, wolfCrypt, elliptic, jsrsasign, python-ecdsa, ruby_ecdsa, fastecdsa, easy-ecc и смарт-карты Athena IDProtect. Потенциально уязвимыми являются карты Valid S/A IDflex V, SafeNet eToken 4300 и TecSec Armored Card, которые используют типовой модуль ECDSA.

Уязвимость связана с возможностью определения значений отдельных битов во время выполнения умножения на скаляр при операциях с эллиптической кривой. Для выделения информации о битах используется такой косвенный метод, как оценка задержки при выполнении вычислений. Для осуществления атаки преступник должен иметь непривилегированный доступ к хосту, на котором выполняется генерация цифровой подписи. Удаленная атака также возможна, однако требует большого объема данных для анализа.

Несмотря на незначительный размер утечки, для ECDSA определения даже нескольких битов с информацией о векторе инициализации (nonce) достаточно для проведения атаки по последовательному восстановлению всего закрытого ключа. По словам авторов метода, успешное восстановление ключа достигается с помощью анализа от нескольких сотен до нескольких тысяч цифровых подписей, сгенерированных для известных атакующему сообщений. Например, для определения закрытого ключа, используемого на смарт-карте Athena IDProtect на базе чипа Inside Secure AT90SC, при использовании эллиптической кривой secp256r1 было проанализировано 11 тысяч цифровых подписей. Общее время атаки составило 30 минут, пишет OpenNet.

Уязвимость исправлена в выпусках libgcrypt 1.8.5 и wolfCrypt 4.1.0, обновление для других проектов еще готовится.

Подробнее: https://www.securitylab.ru/news/501553.php