



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ
Кафедра информационной безопасности

Лабораторная работа №6

Выполнили студенты гр. М9120-
09.04.02ИБКФС

Ефременко И.В.,
Медведев Н.В

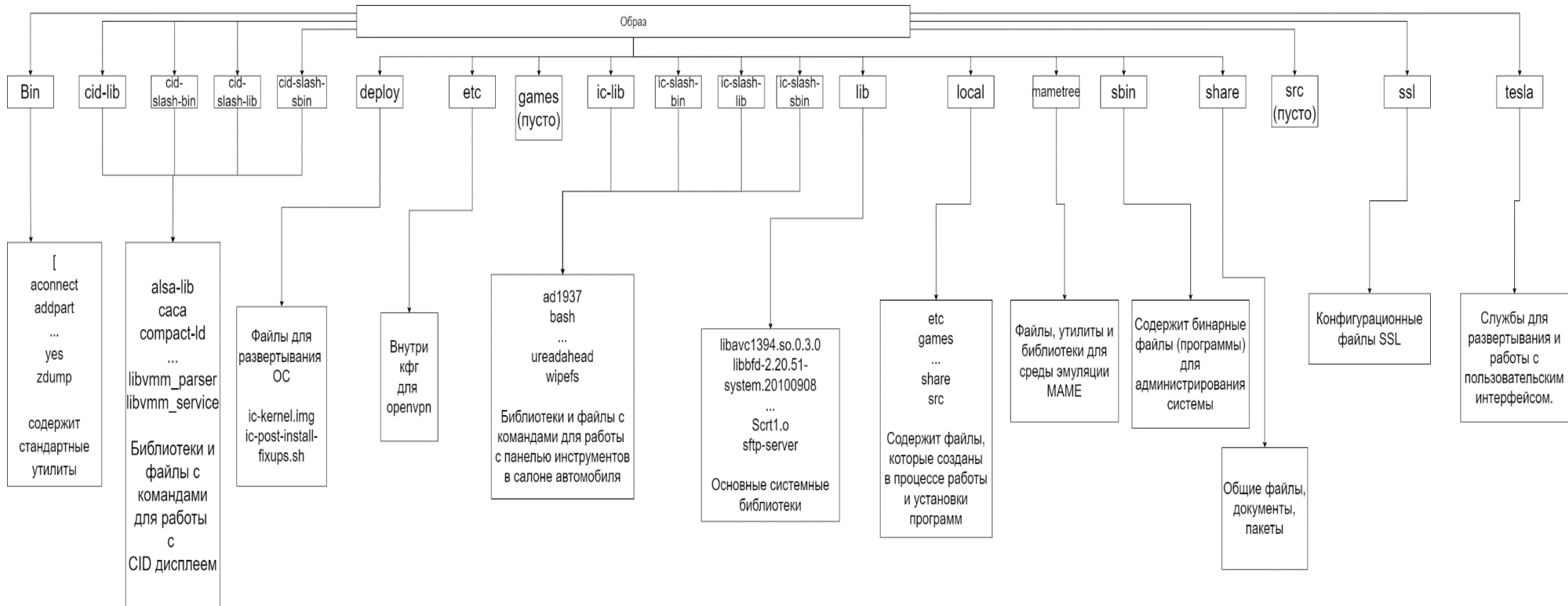
Старший преподаватель

С.С. Зотов

зачтено / не зачтено

г. Владивосток
2022

Дерево образа



В папках tesla и share было найдено множество SSL сертификатов. Их последующая расшифровка дала некоторые данные о том, для кого они были выставлены.

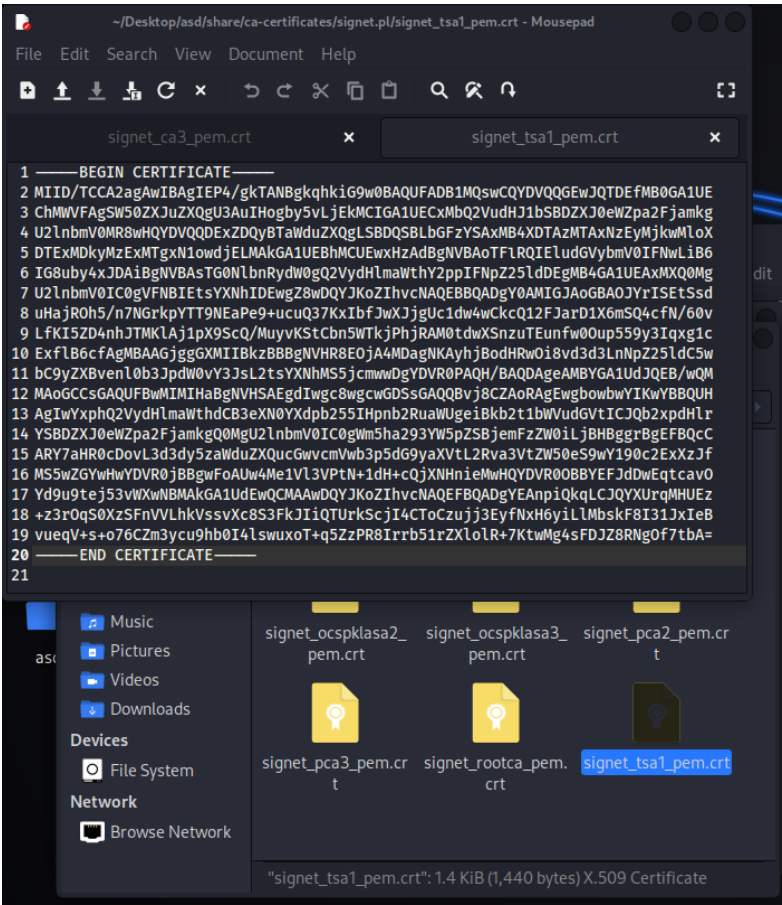


Рисунок 1 Сертификат

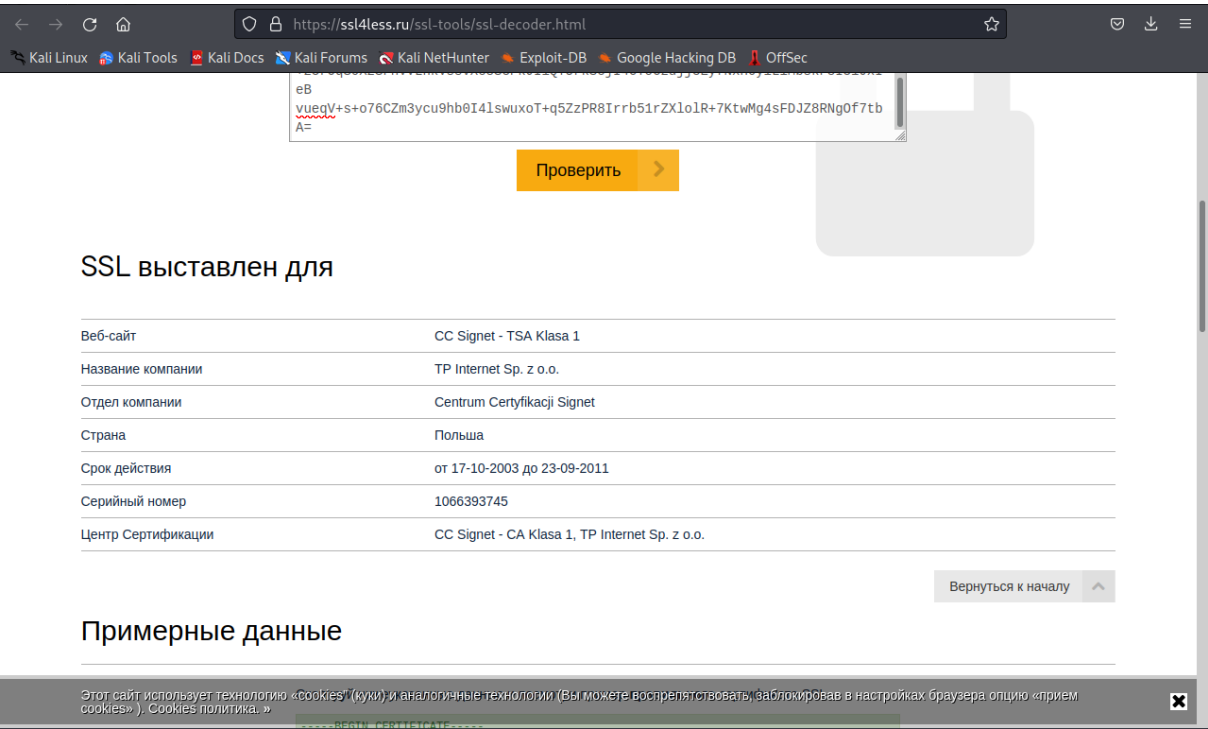
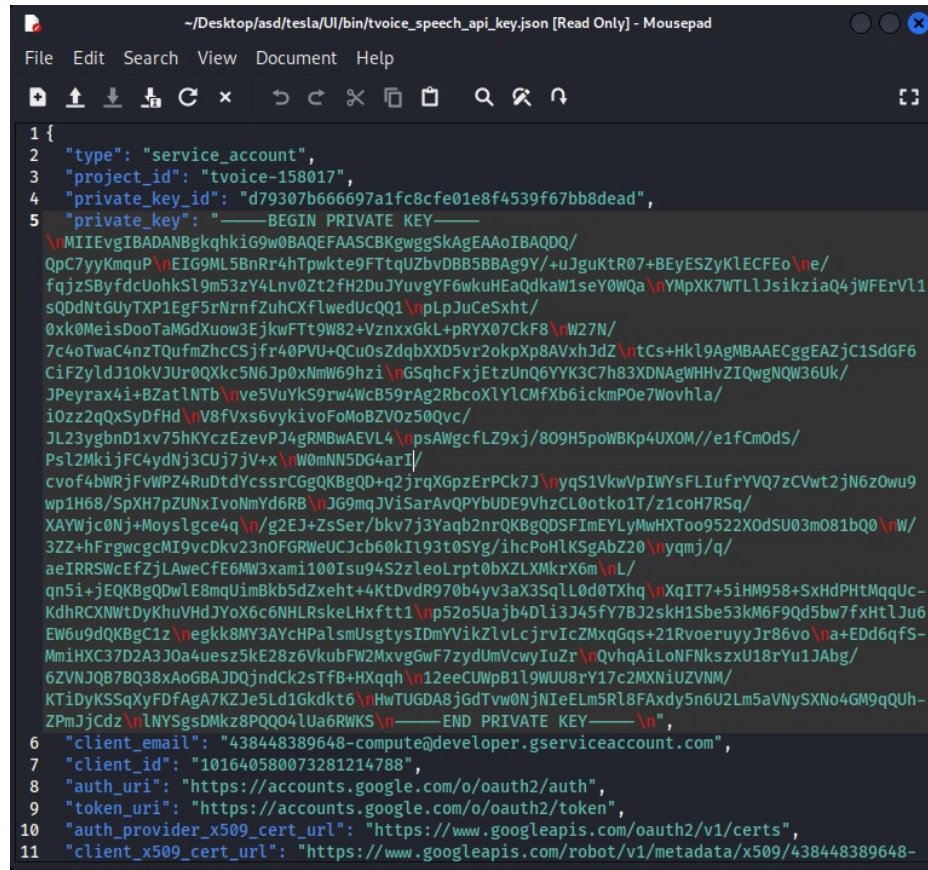


Рисунок 2 Расшифровка

Также были найдены приватные ключи.

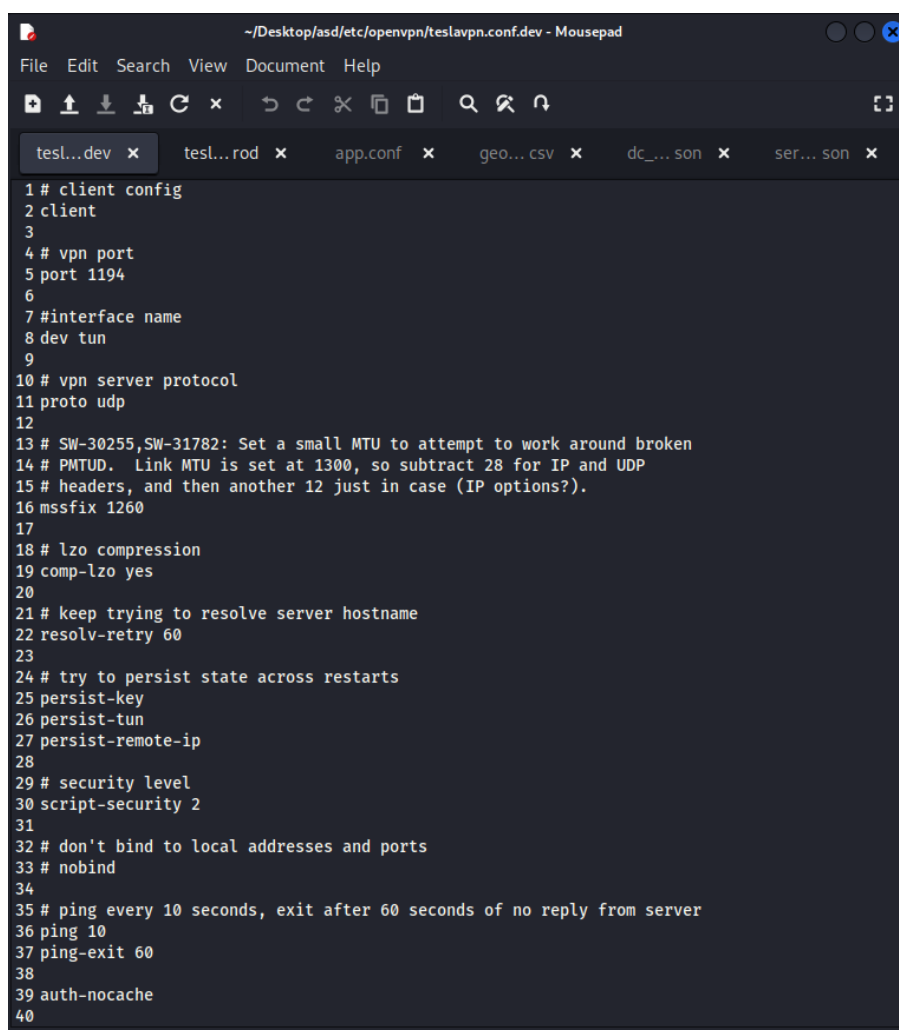


```
1 {
2   "type": "service_account",
3   "project_id": "tvoice-158017",
4   "private_key_id": "d79307b666697a1fc8cfe01e8f4539f67bb8dead",
5   "private_key": "-----BEGIN PRIVATE KEY-----
6   \nMIIIEvgIBADANBgkqhkiG9w0BAQEFAASCBAgEAAoIBAQQD/
7   QpC7yyKmqP\nEIG9ML5BnRr4hTpwkte9FTtqUZbvDBB5BBAG9Y/+uJguKtR07+BEyESZyKLECFEo\nne/
8   fqjzS8yFdcUohkSL9m53zY4Lnv0Zt2fH2DuJYuvyYF6wkuHEaQdkaW1seY0WQa\nYmpXK7WTLlJ3sikziaQ4jWFErVl1
9   sQDdNtGUyTXP1EgF5rNrfZuhCXflwedUcQ1\npLpJuCeSxht/
10  0xk0MeisDooTAMGdXuow3EjkwFTt9W82+VznxxGkL+pRYX07CkF8\nW27N/
11  7c4oTwaC4nzTQufmZhcCSjfr40PVU+QCu0sZdqbXXD5vr2okpXp8AVxhJdZ\nntCs+HkL9AgMBAECggEAEZjC1SdG6F6
12  CiFZyldJ10kVJU0QXkc5N6Jp0xNmW69hzi\nnGSqhcFxFjEtzUnQ6YYK3C7h83XDNAgWHHvZIQwgNQW36UK/
13  JPeyrax4i+BZatlNTb\nve5VuYkS9rw4WcB59rAg2RbcoXLYLCmfXb6ickmPOe7Wovhla/
14  i0zz2qXsYdFhd\nV8fVxs6vykivoFoMoBZV0z50Qvc/
15  JL23ygbnD1xv75hKYczEzevPJ4gRMBwAEVL4\nnpsAWgcFLZ9xj/809H5p0WBKp4UXOM//e1fCmOdS/
16  Psl2MkiJFC4ydNj3CUj7jV+x\nW0mNN5DG4arI/
17  cvof4bWRjFvWPZ4RuDtYcssrCGgQKBgQD+q2jrrXGpZErPCk7J\nnyqS1VkwVpIWYsFLIufYVQ7zCVwt2jN6zOwu9
18  wp1H68/SpXH7pZUNXivoNmYd6RB\nJG9mqJViSarAvQPYbUDE9VhZCL0otko1T/z1coH7RSq/
19  XAYWjc0Nj+Moyslgce4q\n/g2EJ+ZsSer/bkv7j3Yaqb2nrQKBgQDSFImEYLYMwHXToo9522X0dSU03m081bQ0\nrW/
20  3ZZ+hFrgwcgMI9vcDkv23n0FGRWeUCJcb60kIL93t0SYg/ihcPoHLKSgAbZ20\nnyqmj/q/
21  aeIRRSWcEfZjLAweCFE6MW3xami100Isu94S2zLeoLrpt0bXZLXMkrX6m\nnL/
22  qn5i+jEQKBgQDwLE8mqUimBkb5dZxeht+4KtDvdR970b4yv3aX3SgLL0d0TXhq\nXqIT7+5iHM958+SxHdPHTMqqUc-
23  KdhRCXNwtDyKhuVhdJYoX6c6NHLRskeLHxftt1\nnp52o5Uajb4Dli3J45fY7BJ2skH1Sbe53kM6F9Qd5bw7fxHtLJu6
24  EW6u9dQKBGc1z\nnegkk8MY3AYcHPalsmUsgtysIDmYVikZlVLCjrvIcZMxqG6qs+21RvoeryuyJr86vo\nna+EDd6qfS-
25  MmiHXC37D2A3J0a4uesz5kE28z6VkubFW2MxvgGwF7zydUmVcwyIuZr\nQvhqAiLoNFNkszxU18rYu1JAbg/
26  6ZVNJQ87BQ38xAoGBAJDQjndCk2sTfB+HXqgh\n12eeCUWpB19WU08rY17c2MXNiUZVNM/
27  KTiDyKSSqXyFdfAgA7KZJe5Ld1Gkdkt6\nHwTUGDA8jGdTvw0NjNIeELm5R18FAxdy5n6U2Lm5aVnYSXNo4GM9qQUh-
28  ZPmJjCdz\nnLNYSGsDMkz8PQQ04LUa6RWKS\n-----END PRIVATE KEY-----\n",
29   "client_email": "438448389648-compute@developer.gserviceaccount.com",
30   "client_id": "101640580073281214788",
31   "auth_uri": "https://accounts.google.com/o/oauth2/auth",
32   "token_uri": "https://accounts.google.com/o/oauth2/token",
33   "auth_provider_x509_cert_url": "https://www.googleapis.com/oauth2/v1/certs",
34   "client_x509_cert_url": "https://www.googleapis.com/robot/v1/metadata/x509/438448389648-
```

Рисунок 3 Приватный ключ

SSL/TLS-соединения всего этого и многого другого софта уязвимы для широкого спектра MitM-атак («человек посередине»). При этом MitM-атаку можно провести зачастую даже без подделки сертификатов и без похищения приватных ключей, которыми серверы подписывают свои сертификаты. MitM-атаку можно провести, просто эксплуатируя логические уязвимости, которые присутствуют в процедуре проверки SSL/TLS-сертификата на стороне клиентского софта. В результате MitM-злоумышленник может, например, собирать токены авторизации, номера кредитных карт, имена, адреса и прочее — у любого продавца, который использует уязвимые веб-приложения обработки платежей.

Были найдены также данные с точками геолокации. Большинство конечно были просто местами разных отелей и сервисов. Возможно просто карты без личной привязки. А также были найдены конфиги openvpn.

A screenshot of a text editor window titled '~/.Desktop/asd/etc/openvpn/teslavpn.conf.dev - Mousepad'. The window contains a configuration file for an OpenVPN client. The configuration includes settings for the client mode, port (1194), interface (tun), protocol (udp), MTU (1260), compression (lzo), and security level (2). It also includes a ping command and a note about the MTU setting.

```
1 # client config
2 client
3
4 # vpn port
5 port 1194
6
7 #interface name
8 dev tun
9
10 # vpn server protocol
11 proto udp
12
13 # SW-30255,SW-31782: Set a small MTU to attempt to work around broken
14 # PMTUD. Link MTU is set at 1300, so subtract 28 for IP and UDP
15 # headers, and then another 12 just in case (IP options?).
16 mssfix 1260
17
18 # lzo compression
19 comp-lzo yes
20
21 # keep trying to resolve server hostname
22 resolv-retry 60
23
24 # try to persist state across restarts
25 persist-key
26 persist-tun
27 persist-remote-ip
28
29 # security level
30 script-security 2
31
32 # don't bind to local addresses and ports
33 # nobind
34
35 # ping every 10 seconds, exit after 60 seconds of no reply from server
36 ping 10
37 ping-exit 60
38
39 auth-nocache
40
```

Рисунок 4 OpenVPN

Существует 4 уязвимости, связанных с OpenVPN:

CVE-2017-7521 – эта уязвимость классифицируется как удалённый сбой сервера / утечки памяти / двойное освобождение памяти (double-free, один и тот же участок памяти освобождается дважды).

CVE-2017-7520 - эта уязвимость угрожает только тем, кто использует OpenVPN для подключения к прокси NTLM version 2. При использовании возможна утечка данных и потенциальная возможность для атаки MiTM. Пароль пользователя хранится в стеке, и может быть отправлен пиру чистым текстом. Такая атака может быть спровоцирована злоумышленником в дистанционном режиме.

CVE-2017-7508 - уязвимость позволяет осуществить удалённое обрушение сервера, на котором работает OpenVPN, если злоумышленник пошлёт на него специальным образом составленные данные.

CVE-2017-7522 - Атака с обрушением сервера mbed TLS/PolarSSL для своего успешного проведения требует, чтобы на сервере была установлена опция

конфигурации –x509-track. Уязвимости подвержена OpenVPN 2.4 (не 2.3), скомпилированная с криптографическим бэкендом mbed TLS/PolarSSL.

Возможные векторы атаки

CVE-2020-15912

Позволяют злоумышленникам открывать дверь, используя доступ к законной карте-ключу, а затем используя реле NFC.

Для атаки можно воспользоваться приложением NFCCGate и настроить беспроводное устройство для запуска сервера шлюза.

CVE-2020-10558

Допускает отказ в обслуживании из-за неправильного разделения процессов, что позволяет злоумышленникам отключить спидометр, веб-браузер, климат-контроль, визуальные и звуковые сигналы поворотников, навигацию, автопилот. уведомления, а также другие различные функции с главного экрана.

Чтобы воспользоваться уязвимостью, пользователь должен перейти на специально созданную веб-страницу. Эта веб-страница приведет к сбою интерфейса браузера на основе хрома и, по сути, к сбою всего интерфейса Tesla Model 3.

Если вы хотите протестировать его на своем Tesla перед обновлением, не стесняйтесь зайти сюда. Пожалуйста, ведите машину ответственно, так как это не мешает вам управлять автомобилем вручную. Ты все еще можешь водить.