|  |  |
| --- | --- |
| Description | malicious code on the engine ECU through diagnostic reprogramming routine |
| Attack Class | Tampering |
| Attack base | Diagnostic attack |
|  | Integrity |
| affected asset | Information security |
| interface entry point | OBD |
| affected components | ECU, Engine control module |
| tools required | Vehicle diagnostic software, laptop/PC, communication tool, pass through device |
| Requirements | Access/connection to OBD |
| restrictions | Access control, security features, version of diagnostic |
| attack level | Local network |
| acquired priviledges | Full control (functional components) |
| consequence | Malicious code on ECU |
| Rating | 6.7 |
|  | L,L,L,R,C,L,H,N |

|  |  |
| --- | --- |
| Description | deactivation of ECU communication over CAN using diagnostic function |
| Attack Class | Denial of Service |
| Attack base | Diagnostic attack |
| Violated Security Property | Availability |
| affected asset | Reliability |
| interface entry point | OBD |
| affected components | ECU |
| tools required | CAN-to-USB converter, laptop/PC, Arduino, CARSHARK |
| Requirements | Access/connection to OBD |
| restrictions | None |
| attack level | Local network |
| acquired priviledges | Execute (functional component) |
| consequence | ECU communication is disabled |
| Rating | 7.3 |
|  | L,L,L,N,C,N,L,H |

|  |  |
| --- | --- |
| Description | Eavesdropping on CAN network through ECU communication using Arduino sniffer |
| Attack Class | Information disclosure |
| Attack base | Bus attack |
| Violated Security Property | Integrity, confidentiality (?) |
| affected asset | Information |
| interface entry point | OBD |
| affected components | ECU |
| tools required | CAN BUS shield, Arduino, cables, SD card reader, … |
| Requirements | Access/connection to OBD |
| restrictions | Knowledge of arduino |
| attack level | Local network |
| acquired priviledges | Read (functional component) |
| consequence | CAN bus communication and relevant information is leaked |
| Rating | 5.1 |
|  | P,L,N,R,C,N,N,H |

|  |  |
| --- | --- |
| Description | Flooding the CAN network through ECU communication using Arduino |
| Attack Class | Denial of Service |
| Attack base | Flooding attack |
| Violated Security Property | Availability |
| affected asset | Reliability |
| interface entry point | OBD |
| affected components | ECU |
| tools required | CAN BUS shield, Arduino, cables, SD card reader, … |
| Requirements | Access/connection to OBD |
| restrictions | None |
| attack level | Local network |
| acquired priviledges | Execute (functional component) |
| consequence | ECU communication is disabled |
| Rating | 5.3 |
|  | P,L,N,R,C,N,N,H |

|  |  |
| --- | --- |
| Description | Replay attack through car key spoofing, stealing car |
| Attack Class | Spoofing |
| Attack base | Replay Attack |
| Violated Security Property | Integrity |
| affected asset | Information, reliability |
| interface entry point | PKES System |
| affected components | Entire car |
| tools required | Signal transmitter, signal receiver, jammer, phone, … |
| Requirements | Near someone opening their car |
| restrictions | None |
| attack level | Local network |
| acquired priviledges | Full control (functional component) |
| consequence | Car is stolen |
| Rating | 5.1 |
|  | Physical,L,N,R,C,H,L,L |

