|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Type | Element | Description | Impact |
| T1 | Spoofing | 2.1 Get address info | A hack app pretending to be Mapbox API and sends fake address data to “Get address info” | The fake address data may contain harmful code and cause app crash |
| T2 | Spoofing | 4.4 Create contact | A hack app pretending to “Fill in info in ContactManager” and sends fake location and contact data to “Create contact” | The fake data may contain harmful code and cause app crash |
| T3 | Spoofing | User | A hack app pretending to be Contact Manager and creates a fake contact (4.4) which is displayed to the User with either the correct or incorrect contact information as desired by the hacker’s programming. | The fake contact information may be a criminal’s desired meeting place with the User (criminal is a e.g. serial killer, con artist, etc.) instead of the location it should have been. |
| T4 | Tampering | 4.2 Open ContactManager | A snuck malware may modify features of “Open ContactManager”. | Something other than the intended application could be launched (spoof or otherwise) |
| T5 | Tampering | Data flow: from 2.1 Get address info to 2.2 Create marker | A snuck malware may intercept (hooking, etc.) the address info sent by “Get address info”, modify it, and send to “Create marker” | Marker created at wrong location |
| T6 | Tampering | Data flow: from 2.3 Apply style to marker to 2.4 Create popup with info | A snuck malware may modify information about which style is sent by 2.3 or alter the style itself. | The custom style may contain malicious code or use incompatible parameters which crash the application. |