Samsung Pay Vulnerability Reporting

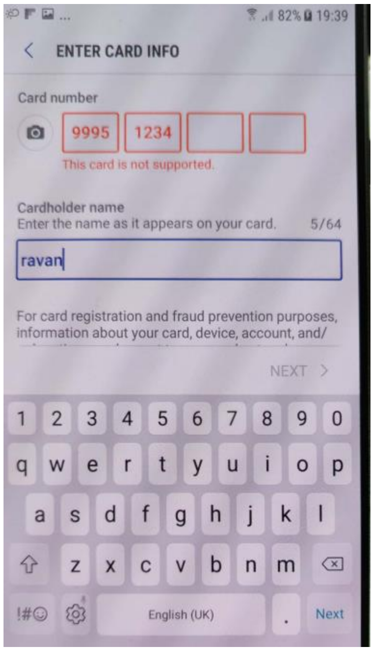
Samsung pay uses Knox platform

- Version: 2.8.49
- Current version: 2.9.33
- Package Name: com.samsung.android.spay
- Vulnerabilities found:
    - Exposure of private information
    - Improper export of Android components

Vulnerabilities found

1. **Exposure of private information (credit card number and cardholder name) :**
    - **Impact description:** Exposure of credit card number and card holder's name can be sniffed by a malicious app with accessibility permission. The leak can lead to financial loss to the customer
    - **Steps to reproduce:**
        - Create an app with accessibility permission and install it in the Samsung device
        - Start the app, the app will intercept all the UI events and store it in a file
        - Open Samsung pay app and got add credit card option and try manual entry of the credit card number
        - After adding the credit card number, check the file created by our app. It will contain the credit card number and the holder's name
    - **Screenshots:**
    - **Available on latest version also**

    - **Impact description:** Several activities in SPay are exported with complete access. But when an attacker tries to launch the activity the app closes automatically and sends an error report. So it is not exploitable
    - **Screenshots**



ENTER CARD INFO

Card number

9995 1234

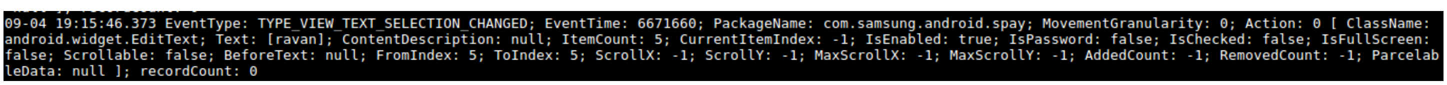
This card is not supported.

Cardholder name

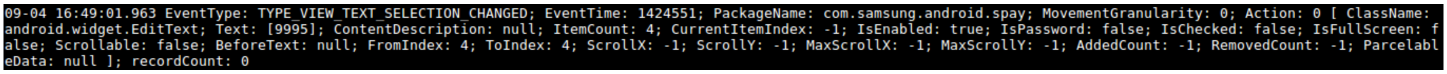
Enter the name as it appears on your card. 5/64

ravan

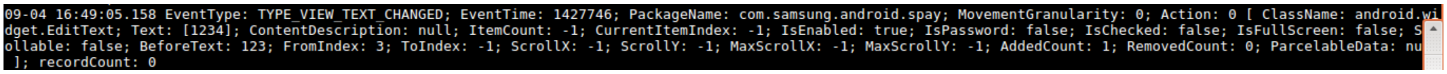
For card registration and fraud prevention purposes, information about your card, device, account, and/



```
09-04 19:15:46.373 EventType: TYPE_VIEW_TEXT_SELECTION_CHANGED; EventTime: 6671660; PackageName: com.samsung.android.spay; MovementGranularity: 0; Action: 0 [ ClassName: 
android.widget.EditText; Text: [ravan]; ContentDescription: null; ItemCount: 5; CurrentItemIndex: -1; IsEnabled: true; IsPassword: false; IsChecked: false; IsFullScreen: 
false; Scrollable: false; BeforeText: null; FromIndex: 5; ToIndex: 5; ScrollX: -1; ScrollY: -1; MaxScrollX: -1; MaxScrollY: -1; AddedCount: -1; RemovedCount: -1; Parcelab
leData: null ]; recordCount: 0
```



```
09-04 16:49:01.963 EventType: TYPE_VIEW_TEXT_SELECTION_CHANGED; EventTime: 1424551; PackageName: com.samsung.android.spay; MovementGranularity: 0; Action: 0 [ ClassName: 
android.widget.EditText; Text: [9995]; ContentDescription: null; ItemCount: 4; CurrentItemIndex: -1; IsEnabled: true; IsPassword: false; IsChecked: false; IsFullScreen: f
alse; Scrollable: false; BeforeText: null; FromIndex: 4; ToIndex: 4; ScrollX: -1; ScrollY: -1; MaxScrollX: -1; MaxScrollY: -1; AddedCount: -1; RemovedCount: -1; Parcelabl
eData: null ]; recordCount: 0
```



```
09-04 16:49:05.158 EventType: TYPE_VIEW_TEXT_CHANGED; EventTime: 1427746; PackageName: com.samsung.android.spay; MovementGranularity: 0; Action: 0 [ ClassName: android.wi
dget.EditText; Text: [1234]; ContentDescription: null; ItemCount: -1; CurrentItemIndex: -1; IsEnabled: true; IsPassword: false; IsChecked: false; IsFullScreen: false; S
ollable: false; BeforeText: 123; FromIndex: 3; ToIndex: -1; ScrollX: -1; ScrollY: -1; MaxScrollX: -1; MaxScrollY: -1; AddedCount: 1; RemovedCount: 0; ParcelableData: nu
 ]; recordCount: 0
```