timebender Technologies India Pvt. Ltd.

24 November 2016

RESPONSIBLE VULNERABILITY DISCLOSURE FOR PAYTM BUG BOUNTY PROGRAM

DESCRIPTION :

Location : POS feature in Paytm app version 5.5.6 .

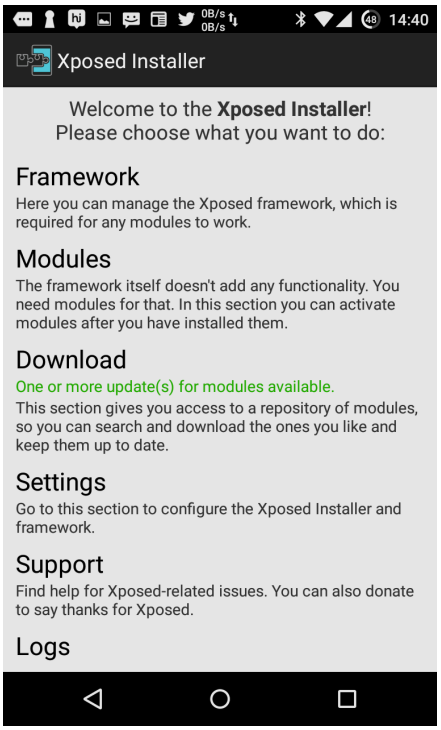
Potential impact : Customer debit card/ credit card data can be stolen in real time.

Summary : With the launch of the new POS (Point of sale) feature in the new Paytm app, vendors can receive payments from customers in their paytm app using credit/debit cards. The customers are asked to trust the devices of the vendors in this mechanism. If the vendor uses compromised devices or if the vendor himself uses malicious apps inside his device, the credit card/debit card details of the customer can be captured in real time.

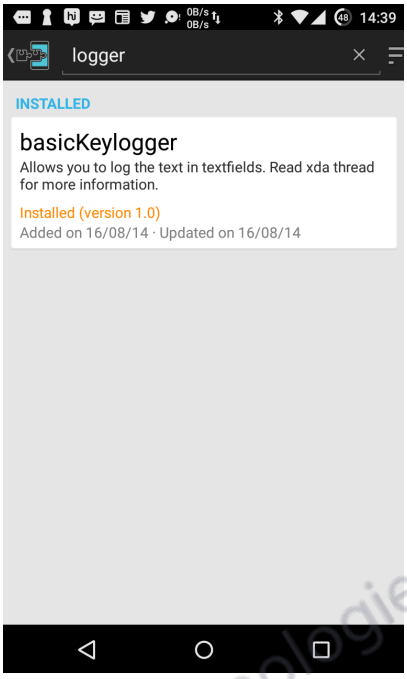
Detailed description :

In this attack vector, the vendor installs malicious apps to log the debit card/ credit card details in his android device. [Test device : Nexus 4, OS : Android lollipop 5.1.1].

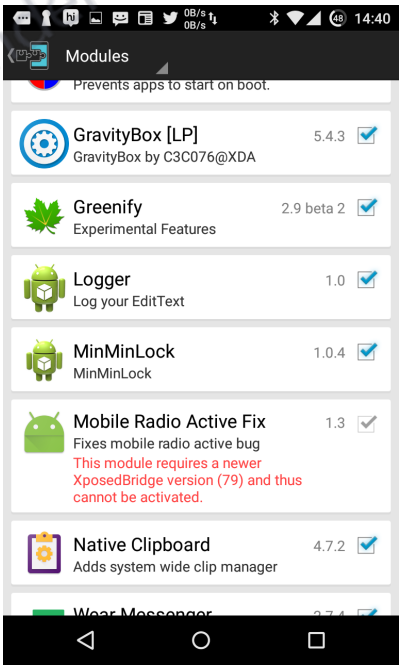
1. Unlock the device boot loader, install the xposed framework.
http://forum.xda-developers.com/showthread.php?t=3034811



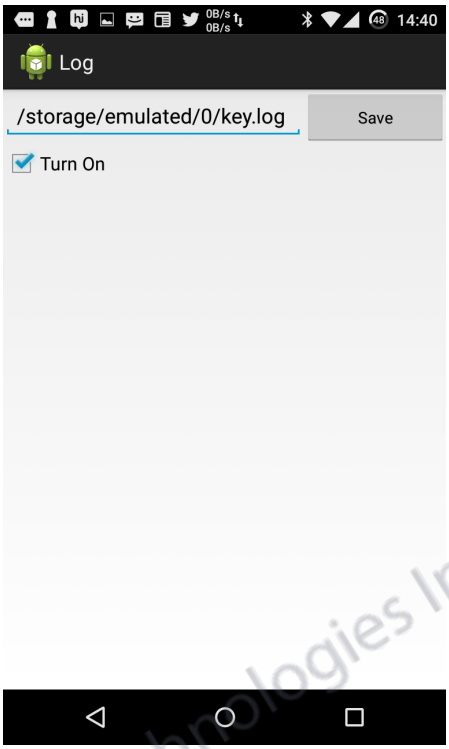
2. Install Logger (basicKeylogger) xposed module.
http://forum.xda-developers.com/xposed/modules/xposed-basickeylogger-logs-textfields-t2849051



3. Enable the Logger xposed module and reboot the device.

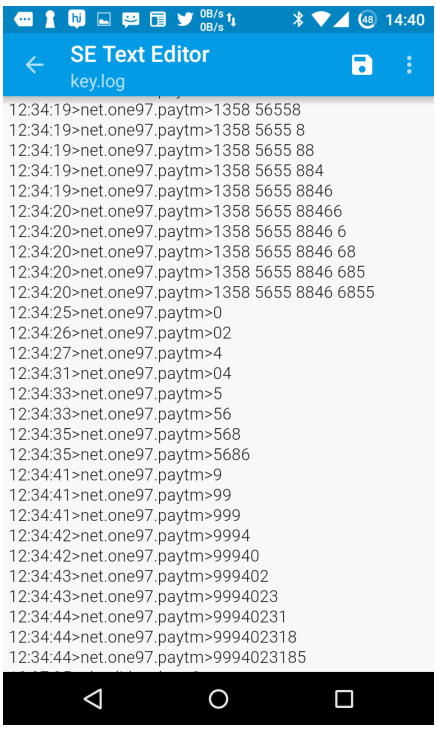


3. Set up the Logger by giving the location of the key.log file.



4. Reboot the device.

5. Everything typed from now onwards, are recorded in the key.log file including the credit card/ debit card details of the customer.



Attached Proof of Concept (POC) video show casing the vulnerability.

Note :
1. This method can also be implemented in a non-rooted android device using system-less xposed framework.
http://forum.xda-developers.com/xposed/unofficial-systemless-xposed-t3388268 .

2. This method can also be implemented on an jailbroken iOS device using appropriate key logging technique.

Mitigation :

1. Don't ask customer to enter credit/debit card details on an un-trusted device. [Recommended].
2. Detect whether the android device has unlocked boot loader (or) rooted (or) both and disable functioning of the paytm app using SafetyNet API on that device.
https://developer.android.com/training/safetynet/index.html
3. Detect whether the iOS device is jailbroken and disable Paytm app on that device - http://stackoverflow.com/a/20505637

Note : Remove jailbroken device techniques from the exclusion list of bounty hunting T&C, as it's no longer valid for POS services.

For more information regarding the vulnerability and for help with mitigation of the vulnerability mail to infosec@timebender.in .

Terms :

1. Contact us within 72 hours from receiving the disclosure of the vulnerability as per the bug bounty program.
2. Fix the vulnerability within 2 days due to severity of the nature of the bug. In case the fix takes longer, keep us posted with the developments as per the bug bounty program.
3. Recognition should be in the name of 'Timebender Technologies' - www.timebender.in .
4. In case the disclosure provided is not being accepted as a vulnerability (or) if any of the above guidelines are not followed (or) both, Timebender Technologies is allowed to make full public disclosure of the said/perceived vulnerability.