nexthardware.com

a cura di: **Ennio Pirolo - SantEnnio - 10-02-2012 12:30**

Trovate falle nella sicurezza di Google Wallet

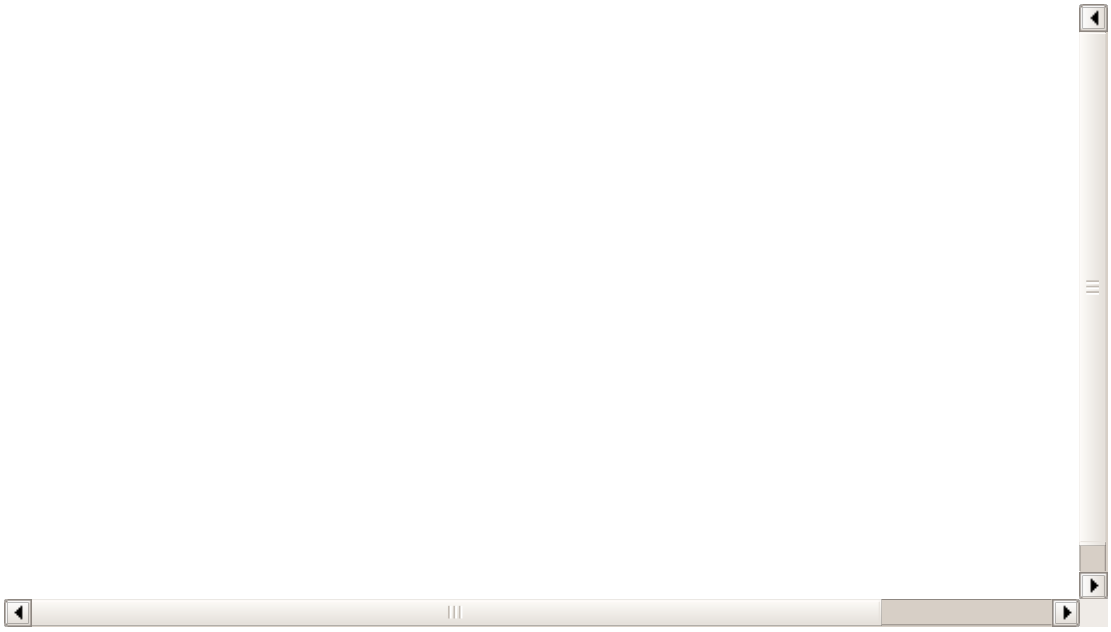
LINK (https://www.nexthardware.com/news/pocketpc-smartphone/4336/trovate-falle-nella-sicurezza-di-google-wallet.htm)

Scovate due vulnerabilità del sistema di pagamento Android.

Qualche tempo fa Google presentò Wallet (/news/pocketpc-smartphone/3957/google-introduce-google-wallet.htm), una app Android che sfrutta il sensore NFC dei telefoni Nexus per effettuare pagamenti con lo smartphone.

Il funzionamento dell'app è estremamente semplice: l'utente sceglie un PIN di quattro cifre al primo accesso e poi ha la possibilità di associare una serie di carte di credito; successivamente basta appoggiare il telefono sul registratore di cassa NFC per effettuare il pagamento.

La delicatezza del compito di questa app non è passata inosservata agli autori dei due hack che vi riportiamo di seguito.



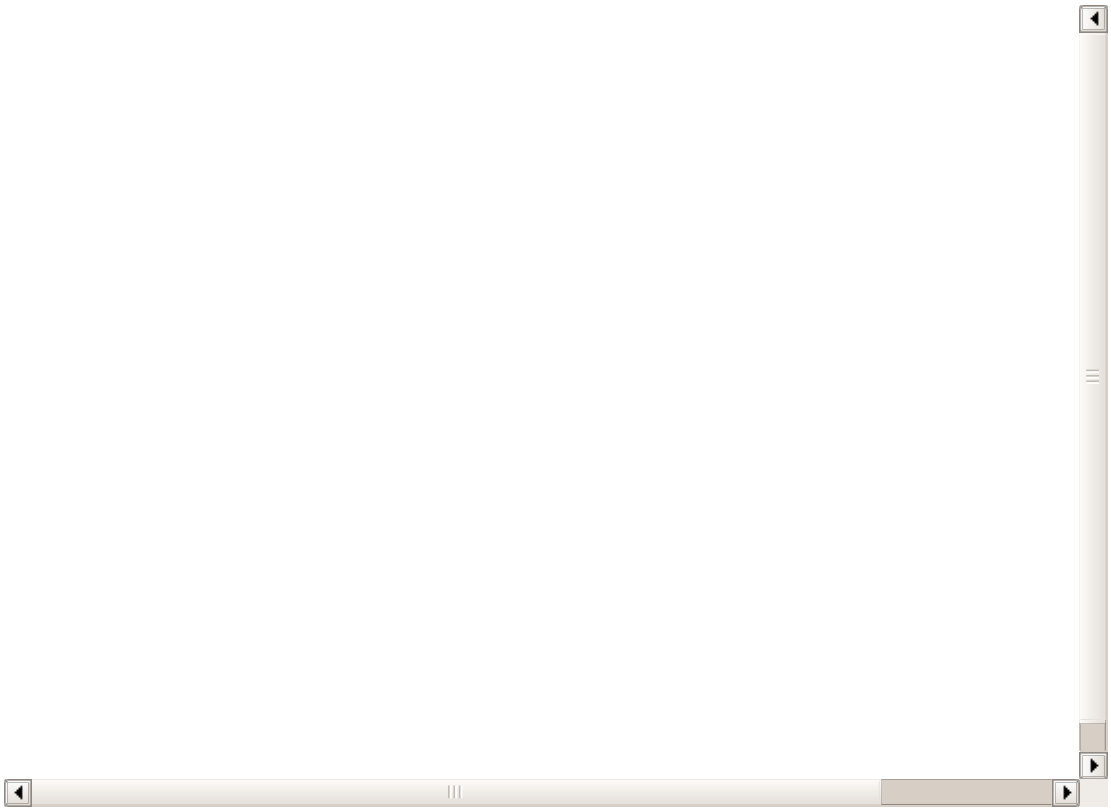
Il primo hack accedeva al database (sqlite3) di Wallet andando ad eseguire un attacco *brute-force* sui dati utente crittografati.

Mentre l'app permette di inserire al massimo 5 volte il PIN, con questo tipo di attacco si possono effettuare tutte le prove che si vogliono e dopo circa 10000 tentativi, che il telefono esegue in pochissimo tempo, si riesce a risalire al codice.

Importante sottolineare che per accedere a questi dati l'utente deve avere i privilegi di root, procedura in generale sconsigliata a tutti gli utenti Android proprio per questi motivi.

Google è stata avvistata ed ha realizzato immediatamente un fix per questa falla.

Il secondo hack non va a toccare il PIN della app ma l'associazione tra Wallet e la carta di credito Google Prepaid Card.



Questa procedura è talmente banale che non richiede applicazioni particolari, né privilegi di root, e può provocare ingenti danni in caso di smarrimento del telefono.

Come si vede nel video basta resettare i dati dell'applicazione, riaprirla settando un nuovo PIN ed associare la carta Google che verrà automaticamente riconosciuta a quella di default senza richiedere credenziali d'accesso.

Anche in questo caso la risposta di Google è stata immediata con la creazione di un numero verde a disposizione di tutti gli utenti che abbiano smarrito il telefono e che sono di fatto soggetti a questa vulnerabilità .