CYBER NEWS

Mobile PoS Vulnerabilities Impact Paypal, Square, SumUp

by Milena Dimitrova | **Last Update:** December 30, 2022 | 0 Comments

An alarming discovery was recently made during the Black Hat conference held in Las Vegas. Security researchers from Positive Technologies reported that vulnerabilities in mPOS (mobile Point-of-Sale) machines allow attackers to take over customer accounts and steal credit card data. Affected vendors include Square, SumUp, iZettle, and PayPal.

As reported by researchers Leigh-Anne Galloway and Tim Yunusov, attackers could alter the amount charged to a credit card. They are also capable of other misdeeds such as forcing customers to use other payment methods, like magstripe. The latter can be compromised

Mobile PoS Vulnerabilities Allow Attackers to Tamper with Values, Transactions

The research team uncovered a number of flaws in endpoint payment systems some of which could lead to MiTM attacks. Other attack vectors built on the exploit of these flaws include **the transfer of arbitrary code via Bluetooth** and mobile apps, as well as tampering with magstripe transactions.

All of these attacks are possible due to the way mPoS systems function – via Bluetooth to connect to mobile apps and then send the data to payment provider servers. By intercepting these communications it becomes possible to manipulate values and obtain access to transaction traffic.

On top of this, attackers can remotely execute code on compromised hosts and gain full access to the operating systems of card readers. The list of malicious activities based on these vulnerabilities is rather long. Attackers can also alter purchases, **change their values** or make some transactions look like they have been declined.

Related Story: Prilex PoS Malware Has Everything Cybercrooks Need

One of the researchers, Leigh-Anne Galloway, explained that:

> *Currently there are very few checks on merchants before they can start using a mPOS device and less scrupulous individuals can, therefore, essentially, steal money from people with relative ease if they have the technical know-how. As such, providers of readers need to make sure security is very high and is built into the development process from the very beginning.*

In addition to the mPoS vulnerabilities, the researchers **also reported two other vulnerabilities**, identified as CVE-2017-17668 and CVE-2018-5717, that impact ATMs manufactured by NCR.

Related posts:

1. **Vulnerabilities in Verifone and Ingenico PoS Devices Could Enable Hackers to Steal and Clone Credit Cards**
Security researchers Aleksei Stennikov and Timur Yunusov recently unearthed vulnerabilities...

2. **$1000 Amazon Gift Card Scam – How to Get Rid of It?** The article will aid you to differentiate between a $1000...

3. **Vulnerabilities in GTP Protocol Impact 5G Networks in Various Attacks** A new report showcases serious vulnerabilities the modern GTP communication...

5. **Protecting Your Data from Physical Theft: the 2020 Guide** When you think of protecting your data, does it occur...

6. **Mobile Malware 2015: Ransomware, Tor and Porn Apps** The end of the year is near, and it's time...

7. **CVE-2021-3970: High-Impact Lenovo Notebook BIOS Vulnerabilities** Three recently disclosed (and patched), high impact BIOS security vulnerabilities...

8. **BetterGuard Mobile Software Review** Android devices have become increasingly more secure and this is...