Research reveals security flaw in Android smartphones

Check Point Research, a provider of cybersecurity solutions globally, revealed a security flaw in Samsung, Huawei, LG, Sony and other Android-based phones that leaves users vulnerable to advanced phishing attacks.

Pankaj Bhula, regional director for Checkpoint in Africa

The affected Android phones use over-the-air (OTA) provisioning, through which cellular network operators can deploy network-specific settings to a new phone joining their network. However, Check Point Research found that the industry standard for OTA provisioning, the Open Mobile Alliance Client Provisioning (OMA CP), includes limited authentication methods.

Remote agents can exploit this to pose as network operators and send deceptive OMA CP messages to users. The message tricks users into accepting malicious settings that, for example, route their Internet traffic through a proxy server owned by the hacker.

Researchers determined that certain Samsung phones are the most vulnerable to this form of phishing attack because they do not have an authenticity check for senders of OMA CP messages. The user only needs to accept the CP and the malicious software will be installed without the sender needing to prove their identity.

Huawei, LG, and Sony phones do have a form of authentication, but hackers only need the International Mobile Subscriber Identity (IMSI) of the recipient to ‘confirm’ their identity. Attackers can obtain a victim’s IMSI in a variety of ways, including creating a rogue Android app that reads a phone’s IMSI once it is installed.

The attacker can also bypass the need for an IMSI by sending the user a text message posing as the network operator and asking them to accept a pin-protected OMA CP message. If the user then enters the provided PIN number and accepts the OMA CP message, the CP can be installed without an IMSI.

“Given the popularity of Android devices, this is a critical vulnerability that must be addressed,” said Slava Makkaveev, security researcher at Check Point Software Technologies.

“Without a stronger form of authentication, it is easy for a malicious agent to launch a phishing attack through over-the-air provisioning. When the user receives an OMA CP message, they have no way to discern whether it is from a trusted source. By clicking ‘accept’, they could very well be letting an attacker into their phone.”

The researchers disclosed their findings to the affected vendors in March. Samsung included a fix addressing this phishing flow in their Security Maintenance Release for May (SVE-2019-14073), LG released their fix in July (LVE-SMP-190006), and Huawei is planning to include UI fixes for OMA CP in the next generation of Mate series or P series smartphones. Sony refused to acknowledge the vulnerability, stating that their devices follow the OMA CP specification.