Sicherheitslücke macht Android-Smartphones anfällig für fortschrittliches SMS-Phishing

Check Point Research entdeckt Schwachstellen unter anderem in Mobilgeräten von Samsung, Huawei, LG und Sony

SAN CARLOS, Kalifornien – 5. September 2019. Check Point Research, die Threat Intelligence-Abteilung von Check Point® Software Technologies Ltd. (NASDAQ: CHKP), einem weltweit führenden Anbieter von Cyber-Sicherheitslösungen, enthüllt eine Sicherheitslücke in Samsung, Huawei, LG, Sony und anderen Android-basierten Smartphones. Die Geräte sind dadurch anfällig für fortschrittliche Phishing-Angriffe.

Die betroffenen Mobiltelefone nutzen OTA-Bereitstellung (Over-the-Air), über die Mobilfunkbetreiber netzwerkspezifische Einstellungen auf ein neues Gerät übertragen können, das ihrem Netzwerk beitritt. Check Point Research stellte jedoch fest, dass der Industriestandard für die OTA-Bereitstellung, das Open Mobile Alliance Client Provisioning (OMA CP), nur begrenzte Authentifizierungsmethoden beinhaltet. Angreifer können dies ausnutzen, um sich als Netzbetreiber auszugeben und irreführende OMA CP-Nachrichten an die Benutzer zu senden. Die Nachricht fordert die Benutzer auf, Einstellungen für ihren Netzwerkbetrieb zu akzeptieren, die aber, beispielsweise, ihren Internetverkehr über einen Proxy-Server des Hackers leiten.

Sicherheitsforscher stellten fest, dass bestimmte Samsung-Telefone für diese Form des Phishing-Angriffs am anfälligsten sind, da sie keine Authentizitätsprüfung für Absender von OMA CP-Nachrichten besitzen. Der Benutzer muss nur die Anfrage akzeptieren und der Schad-Code wird installiert, ohne dass der Absender seine Identität nachweisen muss.

Huawei, LG und Sony Telefone haben zwar eine Form der Authentifizierung an Bord, aber Hacker benötigen nur die International Mobile Subscriber Identity (IMSI) des Empfängers, um ihre Identität selbstständig zu ‚bestätigen'. Angreifer können die IMSI eines Opfers auf verschiedene Arten erhalten, einschliesslich der Erstellung einer betrügerischen Android-App, welche die IMSI eines Telefons ausliest, sobald die Anwendung installiert wurde. Der Angreifer kann sogar die Notwendigkeit einer IMSI umgehen, indem er dem Benutzer eine Textnachricht sendet, in der er sich als Netzbetreiber ausgibt und den Nutzer auffordert, eine PIN-geschützte OMA CP-Nachricht zu akzeptieren. Wenn der Benutzer dann die angegebene PIN-Nummer eingibt, kann der CP ohne IMSI installiert werden.

„Angesichts der Popularität von Android-Geräten ist dies eine kritische Schwachstelle, die behoben werden muss", mahnt Slava Makkaveev, Security Researcher bei Check Point Software Technologies: „Ohne eine stärkere Form der Authentifizierung ist es für einen Cyber-Kriminellen einfach, einen Phishing-Angriff über eine Over-the-Air-Bereitstellung durchzuführen. Wenn der Benutzer eine OMA CP-Nachricht erhält, hat er keine Möglichkeit zu erkennen, ob sie wirklich von einer vertrauenswürdigen Quelle stammt. Wenn der Betroffene auf ‚Akzeptieren' drückt, könnten er unbeabsichtigt einen Angreifer in sein Handy lassen."

Im März gaben die Forscher ihre Ergebnisse an die betroffenen Anbieter weiter. Samsung hat in seinem Security Maintenance Release für Mai (SVE-2019-14073) bereits einen Fix für diesen Phishing-Flow aufgenommen, LG hat seinen Fix im Juli (LVE-SMP-190006) veröffentlicht und Huawei plant, UI-Fixes für OMA CP in die nächste Generation von Smartphones der Mate-Serie oder P-Serie aufzunehmen. Sony weigerte sich, die Schwachstelle anzuerkennen und erklärte, dass ihre Geräte der OMA CP-Spezifikation entsprechen.

Check Point SandBlast Mobile verhindert derartige Man-in-the-Middle- und Phishing-Angriffe, um Geräte vor den genannten schädlichen OMA CP-Nachrichten zu schützen. Um mehr über SandBlast Mobile zu erfahren, besuchen Sie bitte den Check Point Produkt-Eintrag.

Mehr zur Schwachstelle finden Sie im Blog Beitrag des Research-Teams.
Alle Berichte des Check Point Research Team finden Sie unter: https://research.checkpoint.com/

Folgen Sie Check Point Research über:
Blog: https://research.checkpoint.com/
Twitter: https://twitter.com/_cpresearch_

Über Check Point Research
Check Point Research bietet führende Cyber-Bedrohungsinformationen für Check Point Software-Kunden und die grössere Intelligenz-Community. Das Forschungsteam sammelt und analysiert globale Cyber-Angriffsdaten, die auf der ThreatCloud gespeichert sind, um Hacker fernzuhalten und gleichzeitig sicherzustellen, dass alle Check Point Produkte mit den neuesten Schutzmassnahmen aktualisiert werden. Das Forschungsteam besteht aus über 100 Analysten und Forschern, die mit anderen Sicherheitsanbietern, der Strafverfolgung und verschiedenen CERTs zusammenarbeiten.

Über Check Point Software Technologies Ltd.
Check Point Software Technologies Ltd. (www.checkpoint.com) ist ein führender Anbieter von Cyber-Sicherheitslösungen für Unternehmen und Regierungen weltweit. Die Lösungen schützen Kunden vor Cyber-Angriffen der 5. Generation mit einer branchenführenden Fangrate von Malware, Ransomware und anderen gezielten Angriffen. Check Point bietet die mehrstufige Sicherheitsarchitektur ‚Infinity' Total Protection mit Gen V Advanced Threat Prevention, die alle Netzwerke, Clouds und mobilen Operationen eines Unternehmens, sowie die Geschäftsinformationen auf diesen Geräten, vor allen bekannten Angriffen schützt. Check Point liefert zudem das umfassendsten und intuitivsten Single Point of Control Management-System der Branche. Check Point schützt über 100'000 Unternehmen jeder Grösse in der ganzen Welt. Check Point Alps (Schweiz und Österreich) mit Sitz in Zürich und Wien beschäftigt rund 50 Mitarbeitende.

Pressekontakt:
Check Point Software Technologies (Switzerland) AG
Sonja Meindl
Tel: +41 44 316 64 44
E-Mail: smeindl@checkpoint.com

Jenni Kommunikation
Sylvana Zimmermann
Tel: +41 44 388 60 80
E-Mail: sylvana.zimmermann@jeko.com

