Check Point entdeckt Sicherheitslücke in Smartphones von Xiaomi

Die vorinstallierte Sicherheits-App des viertgrössten Smartphone-Anbieters der Welt wies eine schwerwiegende Sicherheitslücke auf

San Carlos, Kalifornien, 4. April 2019 – Die Sicherheitsforscher von Check Point® Software Technologies Ltd. (NASDAQ: CHKP) fanden eine schwerwiegende Sicherheitslücke in Mobilgeräten des chinesischen Herstellers Xiaomi. Ausgerechnet in der vorinstallierten Sicherheits-App ‚Guard Provider', die eigentlich die Nutzer vor Malware schützen soll, fanden die Sicherheitsforscher eine Lücke, die einen Angriff über diese App ermöglicht.

Der Netzwerkverkehr der Xiaomi-Smartphones zu und von der App ‚Guard Provider' war ungesichert, daher hätte sich ein Krimineller mit dem gleichen WLAN-Netzwerk wie das Opfer verbinden und einen Man-in-the-Middle (MiTM)-Angriff durchführen können. Zudem setzt ‚Guard Provider' auf einige Drittanbieter Software Development Kits (SDKs), um verschiedene Sicherheits-Services anzubieten. Die Zusammenführung verschiedener SDKs kann aber zu Schwierigkeiten der Kompatibilität führen, wie die Sicherheitsforscher von Check Point anmahnen.
Ein Angreifer, getarnt als Teil einer SDK-Aktualisierung, hätte so den Schutz vor Malware deaktivieren und jeden beliebigen Rogue-Code injizieren können, um Daten zu stehlen, Ransomware einzubauen oder andere Arten von Malware zu installieren. Eine Sicherheitslösung für Mobilgeräte, deren Komponenten aufeinander abgestimmt sind, wie Check Point SandBlast Mobile, könnte diesen Man-in-the-Middle-Angriff dagegen erkennen und erfolgreich verhindern.

Die Sicherheitslücke wurde vom Hersteller bereits mit einem Patch geschlossen und ab Werk installieren Xiaomi-Smartphones alle Updates automatisch – allerdings lässt sich die Funktion deaktivieren. Die Schwachstelle betrifft alle handelsüblichen Smartphones des chinesischen Herstellers Xiaomi.

Den vollständigen Blog-Beitrag über die Nachforschung (auf Englisch) lesen Sie unter:
https://research.checkpoint.com/vulnerability-in-xiaomi-pre-installed-security-app/

Folgen Sie Check Point auf:
Twitter: http://www.twitter.com/checkpointsw
Facebook: https://www.facebook.com/checkpointsoftware
Blog: http://blog.checkpoint.com
YouTube: http://www.youtube.com/user/CPGlobal
LinkedIn: https://www.linkedin.com/company/check-point-software-technologies

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. Seine Lösungen schützen Kunden vor Cyber-Angriffen der 5. Generation mit einer branchenführenden Fangrate von Malware, Lösegeldforderungen und anderen gezielten Angriffen. Check Point bietet eine mehrstufige Sicherheitsarchitektur mit unserer neuen Gen V Advanced Threat Prevention, die alle Netzwerke, Clouds und mobilen Operationen eines Unternehmens vor allen bekannten Angriffen schützt, kombiniert mit dem umfassendsten und intuitivsten Single Point of Control Management System der Branche. Check Point schützt über 100‘000 Unternehmen jeder Grösse.
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

