Check Point berichtete über Schwachstellen in marktführender Drohnenplattform und ermöglichte es dem Hersteller, die Sicherheit zu erhöhen

Sicherheitslücken ermöglichten den Angreifern Zugriff auf die Nutzerkonten der DJI-Drohne

San Carlos, Kalifornien – 8. November 2018. Sicherheitsforscher von Check Point® Software Technologies Ltd. (NASDAQ: CHKP), einem weltweit führenden Anbieter von Cybersicherheitslösungen, und DJI, der weltweit führende Anbieter von zivilen Drohnen und Luftbildtechnologie, geben Details über eine potenzielle Schwachstelle bekannt, die sich auf die Infrastruktur von DJI hätte auswirken können.

In einem Bericht, der in Übereinstimmung mit dem Bug Bounty Program von DJI vorgelegt wurde, skizziert Check Point Research den Prozess, bei dem ein Angreifer durch eine Schwachstelle möglicherweise Zugang zum Konto eines Benutzers erhalten hätte, die im Rahmen des Benutzeridentifikationsprozesses innerhalb des DJI Forums, einem vom DJI gesponserten Online-Forum über DJI-Produkte, entdeckt wurde. Die Sicherheitsforscher von Check Point haben entdeckt, dass die Plattformen von DJI ein bestimmtes Token verwendeten, um registrierte Benutzer über verschiedene Aspekte des Gebrauchs des Forums hinweg zu identifizieren. Diese Massnahme macht den Identifikationsprozess zu einem bevorzugten Ziel für Hacker, die nach Möglichkeiten suchen, auf die Konten der Nutzer zuzugreifen.

Nutzer, die ihre Flugaufzeichnungen, einschliesslich Fotos, Videos und Flugprotokolle, mit den Cloud-Servern von DJI synchronisiert, sowie Unternehmen, die die DJI FlightHub-Software verwendet haben, die eine Live-Kamera, Audio- und Kartenansicht enthält, hätten gehackt und die Informationen kopiert werden können. Diese Schwachstelle wurde inzwischen gepatcht, und es gibt keine Hinweise darauf, dass sie jemals ausgenutzt wurde.

„Wir begrüssen die Expertise, die Check Points Sicherheitsforscher durch die verantwortungsvolle Offenlegung einer potenziell kritischen Schwachstelle bewiesen haben“, sagt Mario Rebello, Vice President und Country Manager Nordamerika bei DJI. „Das ist genau der Grund, warum DJI das interne Bug Bounty-Programm ins Leben gerufen hat. Alle Technologieunternehmen verstehen, dass die Verbesserung der Cybersicherheit ein kontinuierlicher Prozess ist, der nie endet. Der Schutz der Informationen unserer Benutzer hat für DJI höchste Priorität – und wir verpflichten uns zu einer kontinuierlichen Zusammenarbeit mit verantwortungsvollen Sicherheitsforschern wie Check Point.“

„Angesichts der Popularität von DJI-Drohnen ist es wichtig, dass potenziell kritische Schwachstellen wie diese schnell und effektiv behoben werden, und wir begrüssen es, dass DJI genau das getan hat“, sagt Oded Vanunu, Head of Products Vulnerability Research bei Check Point. „Nach dieser Entdeckung ist es für Unternehmen wichtig zu verstehen, dass sensible Informationen über alle Geräte und Plattformen hinweg verwendet werden können, vor allem, wenn sie dann auch noch auf einer Cloud-Plattform bereitgestellt werden und jedem schutzlos ausgeliefert sind, der sich darauf Zugriff verschafft. Darüber hinaus kann es für Unternehmen zu einer Beeinträchtigung der eigenen globalen Infrastruktur führen, wenn sich Angreifer aufgrund der Informationen aus der dortigen Infrastruktur Zugriff darauf verschaffen.“

Die DJI-Ingenieure haben den von Check Point vorgelegten Bericht überprüft und ihn in Übereinstimmung mit der Bug Bounty Policy als hohes Risiko mit geringer Erkennungswahrscheinlichkeit eingestuft. Dies ist auf eine Reihe von Voraussetzungen zurückzuführen, die erfüllt sein müssen, bevor ein potenzieller Angreifer sie nutzen kann. DJI-Kunden sollten immer die aktuellste Version der DJI GO oder GO 4 Pilot-Apps verwenden.

Check Point und DJI empfehlen allen Nutzern, beim digitalen Informationsaustausch wachsam zu bleiben. Nutzer sollten stets vorsichtig sein, wenn sie mit anderen Parteien online zusammen arbeiten und Informationen auf Cloud-Plattformen hochladen. Sie sollten die Rechtmässigkeit von Links in E-Mails und Nachrichten in Frage stellen, die sie in Benutzerforen und Websites erhalten.

Eine komplette Analyse dieser Schwachstelle ist im Check Point Research Blog unter folgendem Link verfügbar: https://research.checkpoint.com/dji-drone-vulnerability/

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 DJI
DJI ist weltweit führend in der Entwicklung und Herstellung von zivilen Drohnen und Luftbildverarbeitungstechnologien für den persönlichen und beruflichen Gebrauch. DJI wurde und wird von Menschen mit einer Leidenschaft für ferngesteuerte Hubschrauber und Experten für Flugsteuerungstechnik und Kamerastabilisierung gegründet und geleitet. Das Unternehmen hat sich zum Ziel gesetzt, Luftbild- und Filmtechnik sowie Plattformen für Erschaffer und Innovatoren auf der ganzen Welt zugänglicher, zuverlässiger und benutzerfreundlicher zu machen. Die globalen Aktivitäten von DJI erstrecken sich derzeit über Nord- und Südamerika, Europa und Asien. Seine revolutionären Produkte und Lösungen wurden von Kunden in über 100 Ländern für Anwendungen in den Bereichen Filmherstellung, Bauwesen, Inspektion, Notfallhilfe, Landwirtschaft, Umweltschutz und vielen anderen Branchen ausgewählt.

Für mehr Informationen besuchen Sie bitte folgende Web-Ressourcen:
Website: www.dji.com
Online Store: store.dji.com/
Facebook: www.facebook.com/DJI
Instagram: www.instagram.com/DJIGlobal
Twitter: www.twitter.com/DJIGlobal
LinkedIn: www.linkedin.com/company/dji

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, Ransomware und anderen gezielten Angriffen. Check Point bietet eine mehrstufige Sicherheitsarchitektur mit der neuen Gen V Advanced Threat Prevention, die alle Netzwerke, Clouds und mobilen Devices 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 40 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

