**Badacze firmy Check Point zaraportowali podatności w wiodącej platformie kontroli nad dronami, umożliwiając wzmocnienie zabezpieczeń**

**Luki w zabezpieczeniach stwarzały możliwość przejęcia kont użytkowników DJI Drone przez hakerów**

**Badacze firmy** [**Check Point® Software Technologies Ltd.**](https://www.checkpoint.com/)**, wiodącego światowego dostawcy rozwiązań z zakresu cyberbezpieczeństwa wraz z DJI – liderem w produkcji dronów cywilnych, podzielili się z opinią publiczną informacjami o potencjalnych podatnościach, które jeśli zostałyby wykorzystane, mogły mieć istotny wpływ na infrastrukturę DJI.**

W raporcie przedłożonym zgodnie z programem DJI Bug Bounty Program, badacze Check Pointa zarysowali proces, w którym atakujący mógł potencjalnie uzyskać dostęp do konta użytkownika poprzez lukę odkrytą w procesie identyfikacji użytkownika w ramach „Forum DJI”, będącego sponsorowanym przez DJI forum online na temat produktów firmy. Badacze Check Pointa odkryli, że platformy DJI używają tokena do identyfikowania zarejestrowanych użytkowników w różnych aspektach tzw. customer experience, co czyniło je celem dla hakerów szukających sposobów na dostęp do kont.

Użytkownicy DJI, którzy zsynchronizowali swoje rekordy lotów, w tym zdjęcia, filmy i dzienniki lotów z serwerami chmurowymi DJI, a także użytkownicy korporacyjni DJI, którzy używali oprogramowania DJI FlightHub, które zawiera m.in. widoki kamery na żywo, dźwięku i mapy, mogli być podatni na ataki. Jak zapewniają firmy, luka ta została już naprawiona i nie ma dowodów, że kiedykolwiek została wykorzystana.

„Cieszymy się, że badacze Check Point wykazali się profesjonalizmem poprzez odpowiedzialne ujawnienie potencjalnej podatności na zagrożenia", powiedział Mario Rebello, wiceprezes i Country Manager w Ameryce Północnej w DJI. "To jest właśnie powód, dla którego DJI stawia program Bug Bounty Program na pierwszym miejscu. Wszystkie firmy technologiczne rozumieją, że wzmacnianie bezpieczeństwa cybernetycznego jest procesem ciągłym, który nigdy się nie kończy. Ochrona integralności informacji naszych użytkowników jest dla DJI najwyższym priorytetem i jesteśmy zaangażowani w dalszą współpracę z badaczami bezpieczeństwa, takimi jak Check Point".

"Biorąc pod uwagę popularność dronów DJI, ważne jest, aby potencjalnie krytyczne podatności, takie jak ta, zostały rozwiązane szybko i skutecznie. I za to skuteczne działanie należy pochwalić DJI" - powiedział Oded Vanunu, kierownik działu badań nad podatnością produktów w Check Point. "Ważnej jest, by organizacje zrozumiały, iż poufne informacje mogą być używane między wszystkimi platformami, a jeśli zostaną ujawnione na jednej z nich, mogą doprowadzić do zagrożenia w globalnej infrastrukturze."

Inżynierowie DJI dokonali przeglądu raportu przedstawionego przez Check Point i zgodnie z polityką dotyczącą błędów wystawiających go na ryzyko, określili je jako wysokie ryzyko / małe prawdopodobieństwo. Wynika to z zestawu warunków wstępnych, które należy spełnić, zanim potencjalny napastnik będzie mógł go wykorzystać. Klienci DJI powinni jednakże zawsze używać najnowszej wersji aplikacji pilotażowych DJI GO lub GO 4.

Check Point i DJI zalecają wszystkim użytkownikom zachowanie ostrożności przy wymienianiu danych cyfrowych. Należy zawsze przestrzegać bezpiecznych praktyk sieciowych oraz stosować zasadę ograniczonego zaufania do linków udostępnianych na forach i stronach internetowych.

Pełna analiza techniczna podatności jest dostępna na blogu firmy Check Point: <https://research.checkpoint.com/dji-drone-vulnerability/>