**Guacamole podatne na ataki**

**Jedna z najpopularniejszych na świecie infrastruktur informatycznych do pracy zdalnej – Guacamole – posiada poważne luki bezpieczeństwa - ujawniają eksperci firmy Check Point. Hakerzy mogli podsłuchiwać sesje zdalne, rejestrować używane hasła i kontrolować komputery w organizacji. Eksperci wskazali dwa wektory ataku, które mogły prowadzić do pełnej kontroli nad całą siecią organizacji.**

Badacze firmy Check Point wykryli luki w zabezpieczeniach Apache Guacamole - czołowej infrastrukturzy informatycznej do pracy zdalnej. Oprogramowanie, które zostało pobrane przez ponad 10 milionów użytkowników na świecie (jest bezpłatne i otwarte) umożliwia pracownikom zdalny dostęp do firmowych sieci komputerowych z dowolnego miejsca za pomocą przeglądarki internetowej. Apache Guacamole działa na wielu urządzeniach, w tym na telefonach komórkowych i tabletach.

Eyal Itkin, jeden ze specjalistów pracujących w firmie Check Point wykazał, że osoba atakująca z dostępem do komputera wewnątrz organizacji może wykonać atak odwrotnego RDP, czyli protokołu pulpitu zdalnego, w którym zdalny komputer zainfekowany złośliwym oprogramowaniem przejmuje dane klienta, który próbuje się z nim połączyć. Tego typu atak umożliwiłby hakerowi kontrolę nad bramą Apache Guacamole, która obsługuje wszystkie sesje zdalne w sieci.

Po uzyskaniu dostępu do bramy, haker może podsłuchiwać wszystkie przychodzące sesje, rejestrować używane poświadczenia, a nawet kontrolować inne sesje w organizacji. Badacze Check Pointa przyznają, że w praktyce oznacza to uzyskanie pełnej kontroli nad całą siecią organizacyjną.

Luki w Guacamole pozwalają na przeprowadzenie ataków na dwa różne sposoby: **Scenariusz odwrotnego ataku:** Zaatakowana maszyna w sieci korporacyjnej wykorzystuje przychodzące połączenie, aby zaatakować bramę Apache, starając się ją przejąć. Drugi to **scenariusz dotyczący nieuczciwego pracownika:** pracownik używa komputera w sieci, aby wykorzystać połączenie na obu końcach i przejąć kontrolę nad bramą.

- *Choć w tych trudnych czasach globalne przejście do zdalnej pracy staje się koniecznością, musimy zdawać sobie sprawę z konsekwencji, jakie zdalne połączenia mają dla bezpieczeństwa. Nasi badacze wykryli kolejne luki, które zagrażają bezpieczeństwu firm i ich pracownikom. Firmy oraz różnego rodzaju organizacje powinny zwrócić szczególną uwagę na zabezpieczenie urządzeń końcowych oraz sieci własnych, a także zaktualizowanie usług pozwalających na pracę zdalną –* mówi Wojciech Głażewski, Country Manager Check Pointa w Polsce.

31 marca Check Point Research ujawnił swoje ustalenia firmie Apache. Nowa, załatana wersja Apache Guacamole została wydana w czerwcu 2020 r.