

KOLEJNE PROBLEMY POPULARNYCH KOMUNIKATORÓW - ZNALEZIONO WINNEGO?

Komunikatory takie jak Slack, Skype i WhatsApp zbudowane z użyciem platformy Electron podatne są na wbudowanie w nie tzw. tylnych drzwi (backdoorów) umożliwiających modyfikację całego oprogramowania - podał w czwartek serwis Ars Technica.

Platforma Electron często wykorzystywana jest przez programistów do tworzenia aplikacji do komunikacji w internecie. Według badacza cyberbezpieczeństwa Pavla Tsakalidisa Electron może być łatwo zhakowany przez potencjalnych cyberprzestępców. Demonstrację takiej operacji Tsakalidis przedstawił podczas konferencji BSides w amerykańskim Las Vegas.

Według eksperta w bibliotece kodu JavaScript i wbudowane rozszerzenia do przeglądarki Chrome platformy Electron można łatwo wstrzyknąć nowy kod, który pozwoli hakerom na zmodyfikowanie działania całego programu stworzonego w oparciu o tę platformę. Dodatkowo, jak argumentuje specjalista, żadne działania hakerów nie są sygnalizowane przez aplikację użytkownikowi, wobec czego pozostaje on nieświadomy manipulacji. Zmodyfikowane oprogramowanie może pozwalać atakującym m.in. na wykradanie wrażliwych danych, przejmowanie kontroli nad kamerką wbudowaną w komputer, a także gromadzenie informacji o przeglądanych stronach internetowych. Jednakże, jak podkreślił ekspert, do wykorzystania podatności Electrona niezbędny jest lokalny dostęp do aplikacji i nie można przeprowadzić tej operacji zdalnie.

Tsakalidis poinformował, że skontaktował się z twórcami platformy Electron, aby powiadomić ich o wykrytej podatności. Nie otrzymał jednak odpowiedzi od firmy.

Jedną z aplikacji rozwijanych w oparciu o platformę Electron - komunikator WhatsApp należący do Facebooka, zawiera również inną podatność bezpieczeństwa, o której poinformowała izraelska firma Check Point Software. Według jej specjalistów hakerzy mogą manipulować treścią wiadomości przesyłanych przez WhatsAppa zarówno w ramach prywatnych rozmów jak i konwersacji grupowych bez pozostawiania śladów widocznych dla korzystających z programu osób, co naraża użytkowników na dezinformację płynącą ze źródeł, które wydawały się zaufane i sprawdzone.

Check Point poinformował, iż podatność ta istnieje od ubiegłego roku, ale WhatsApp zneutralizował jedynie część nieprawidłowości w działaniu aplikacji. Firma oświadczyła też, że współpracuje z WhatsAppem przy rozwiązaniu pozostałych problemów, ale jest to trudne ze względu na metody szyfrowania stosowane w aplikacji.