Domofony Hikvision pozwalają na szpiegowanie sąsiadów

Kristina Beek, Zastępca Redaktora, Dark Reading
21 września 2023
https://www.darkreading.com/ics-ot-security/hikvision-intercoms-snooping-neighbors/

Systemy domofonowe są powszechnie stosowane w tysiącach mieszkań i instytucji jak świat szeroki, jednak niektóre z nich mogą służyć do szpiegowania sąsiadów poprzez inne aparaty w lokalach.
Szczególną uwagę zwrócił w ostatnich czasach możliwy cyberatak przez urządzenia IoT - taki, który za pomocą domofonów Hikvision umożliwia szpiegowanie sąsiadów.
W niedawno publikowanych informacjach badacze z australijskiej firmy Skylight Cyber (https://skylightcyber.com/) ostrzegli, iż potencjał tych urządzeń do ataków szpiegowskich powinien być poważnie wzięty pod uwagę przez rozmaite organizacje gdyż posiada zdolność naruszania prywatności.
(https://www.darkreading.com/endpoint-security/the-privacy-war-is-coming).

Do opisanych niżej badań wybrano chińskie urządzenia Hikvision z uwagi na ich dostępność i stopień rozpowszechnienia. Badacze skupili się na dwóch typach : DS-KH6210-L oraz DS-KH6320-WTE1. Urządzenia były testowane w lokalu mieszkalnym celem zaobserwowania ich zachowania względem innych, pozostałych urządzeń zamontowanych w typowym obiekcie mieszkalnym jako system wideodomofonowy. Skonfigurowano dublowanie portu (Port Mirroring) celem przechwycenia całego ruchu wchodzącego i wychodzącego z urzadzenia domofonowego.

Schemat Scenariusza Włamań

Badania pokazały, iż dokonanie samego tylko ataku nie jest znaczącą trudnością (dokladny opis procedury jest tutaj : https://skylightcyber.com/2023/09/14/neighbourhood-watch-hikvision-intercom-eavesdropping/).
Według specjalistów ze Skylight Cyber potencjalny haker nie potrzebuje wielu narzędzi do przeprowadzenia ataku.
Jak mówi Adi Ashkenazy, szef Skylight Cyber, atakujący potrzebuje jedynie dostępu do danego obiektu. Jeśli obiekt nie jest podłączony do internetu wystarczy dowolny dostęp fizyczny np. z któregokolwiek lokalu w budynku.

W języku technicznym oznacza to jedynie konieczność posiadania laptopa, kabla sieciowego i śrubokręta, dalsza wiedza konieczna do przeprowadzenia ataku jest stosunkowo niska. Tak więc, w sytuacji gdy w obiekcie są zainstalowane domofony Hikvision i zachodzi potrzeba z którejkolwiek strony by dokonać aktu szpiegowania wystarczy odłączyć urządzenie w lokalu (np. wideomonitor), a w jego miejsce podłączyć się laptopem by uzyskać dostęp.

Następnie atakujący uruchamia skrypt pobrany z platformy Github dla złamania hasła administratora w dowolnym aparacie celem uzyskania dostępu do tegoż aparatu domofonowego w dowolnym lokalu. Gdy nastąpi złamanie hasła administratora atakujący loguje się do docelowego aparatu i usuwa kolejne progi zabezpieczeń. Uruchamiając jedną komendę na swoim laptopie, atakujący uzyskuje pełen dostęp wszystkich funkcji aparatu w lokalu, **włącznie z jego mikrofonem.**

Znaczenie oprogramowania szpiegującego

Gdy atakującemu uda się za pomocą kabelka, laptopa i śrubokręta dostać do hasła administratora i złamać progi zabezpieczające obszary chronione, kolejnym najgorszym elementem tego scenariusza jest **uruchomienie mikrofonu w aparacie.**
Jak mówi Adi Ashkenazy : gdy masz już dostęp na tym poziomie masz możliwość **NIEOGRANICZONEGO PODSŁUCHU** dowolnej osoby w dowolnym lokalu budynku, w którym taki aparat domofonowy jest zainstalowany.
Hikvision wprowadził wprawdzie poprawkę zwiększającą poziom zabezpieczenia jednakowoż nadal istnieje wiele przeszkód w jego zastosowaniu. Zabezpieczenie to bowiem obejmuje jedynie kwestie autoryzacyjne, pozostawiając nadal drogi obejściowe.

Co więcej, właściciel lokalu nie jest w stanie dokonać takiej poprawki samodzielnie gdyż nie posiada hasła administratora, więc dokonać tego może jedynie personel producenta w sposób ręczny. Można się więc śmiało założyć, iż mnóstwo obiektów z tym sprzętem pozostanie bez jakiegokolwiek zabezpieczenia.

Reasumując, osoby korzystające z urządzeń wideodomofonowych mają możliwość zmniejszenia ryzyka bezpieczeństwa urządzeń IoT, bądź to współpracując z odpowiedzialnymi dostawcami z reputacją i śledząc architekturę zabezpieczeń produktów, bądź upewniając się że produkty te mają REGULARNIE odświeżany system zabezpieczenia.
Jak dodaje Skylight Cyber : można śmiało stwierdzić, iż obecnie na świecie istnieją tysiące użytkowanych mieszkań gdzie występuje możliwość uruchomienia podsłuchu.