**Wykryto luki zero-day w milionach urządzeń internetu rzeczy z systemem operacyjnym FreeRTOS**

**Ori Karliner, badacz zajmujący się bezpieczeństwem sieciowym, wykrył 13 krytycznych luk bezpieczeństwa w systemie operacyjnym czasu rzeczywistego FreeRTOS. Jest to popularny system instalowany w milionach dostępnych na rynku urządzeń internetu rzeczy. Do zalet FreeRTOS zalicza się zwięzły i czytelny kod oraz niskie zapotrzebowanie na moc obliczeniową.**

System operacyjny FreeRTOS został przyjęty przez Amazon i dalej jest rozwijany jako AWS FreeRTOS. Celem projektu jest stworzenie uniwersalnej platformy programistycznej dla urządzeń IoT, zapewniającej bezpieczną transmisję danych, prosty mechanizm aktualizacji OTA (over-the-air), podpisywanie kodu w celu uwierzytelniania instalowanych aplikacji, wsparcie dla AWS (chmury obliczeniowej Amazonu) i więcej.

FreeRTOS pozwala programistom na szybkie wdrażanie innowacji w segmencie urządzeń IoT, znacząco redukując koszty związane z ich rozwojem. Niestety, w tym przypadku wygoda wiąże się z wysokimi kosztami wynikającymi ze słabych zabezpieczeń.

Luki bezpieczeństwa zostały odkryte w FreeRTOS do wersji V10.0.1 (z protokołem TCP), AWS FreeRTOS do wersji 1.3.1, oraz WHIS OpenRTOS (z komponentem WHIS Connect TCP/IP).

Cztery z odkrytych luk umożliwiają zdalne wykonanie kodu na atakowanym urządzeniu, jedna pozwala stworzyć z urządzeń IoT botnet DDOS (odmowa usługi), a siedem pozostałych może zostać wykorzystanych do kradzieży poufnych danych.

Keliner razem z zespołem zajmującym się testowaniem zabezpieczeń ujawnił błędy w sposób odpowiedzialny, bez podania metody przeprowadzenia ataku, dając producentowi FreeRTOS czas na załatanie odkrytych luk.

„Ponieważ jest to projekt typu open source, daliśmy producentowi FreeRTOS 30 dni na wydanie stosownych łat zabezpieczających, zanim ujawnimy szczegółowe informacje dotyczące wykrytych luk. Aktualnie, w ścisłej współpracy z Amazonem, pracujemy nad poprawkami zabezpieczającymi” – potwierdził zespół Karlinera.

Amazon już załatał kilka z odkrytych luk bezpieczeństwa w komponencie WHIS.

„Ilość urządzeń podłączonych w ramach IoT na całym świecie wzrasta. Ma to zapowiadać nową erę produktywności i wydajności sektora przemysłowego, publicznego, a także zapewniać konsumentom szereg nowych interaktywnych produktów. Należy pamiętać, że wraz ze wzrostem liczby urządzeń podłączonych w ramach IoT rośnie liczba zagrożeń z tym związanych. Urządzenia te, takie jak wirtualni asystenci, zabawki i smartwatche mogą narażać ludzi i ich sieci domowe na ataki, a całe społeczeństwo może być narażone na ataki cybernetyczne na dużą skalę” komentuje Dariusz Woźniak, inżynier techniczny Bitdefender z firmy Marken.