

Bitdefender®

# Google planuje wzmocnienie oprogramowania układowego w celu zwiększenia bezpieczeństwa ekosystemu Androida

23.02.2023

Google podejmuje kroki w celu wzmocnienia bezpieczeństwa ekosystemu Androida poprzez modernizację oprogramowania układowego, będącego cyfrowym kamieniem węgielnym wielu nowoczesnych urządzeń. Czy dzięki temu ruchowi Android zbliży się do poziomu bezpieczeństwa, który oferuje iOS?

Czym jest oprogramowanie układowe?

Google planuje wzmocnienie oprogramowania układowego w celu zwiększenia bezpieczeństwa ekosystemu Androida

Bitdefender®

System operacyjny Android (Android OS) działa na wielordzeniowym procesorze, powszechnie nazywanym procesorem aplikacji (AP).

Chociaż ma to decydujące znacznie znaczenie, AP nie jest jedynym procesorem System on Chip (SoC). Niektóre procesory SoC mają bardziej wyspecjalizowane role, takie jak przetwarzanie multimediów, zapewnianie bezpieczeństwa urządzeniom i przekazywanie komunikacji komórkowej.

Oprogramowanie układowe to suma wszystkich składników oprogramowania, które działają na wyżej wspomnianych dodatkowych procesorach typu System on Chip (SoC). Od kilku lat eksperci do spraw cyberbezpieczeństwa skupiają swoją uwagę na mniej widocznych komponentach oprogramowania. Firma Google też postanowiła wzmocnić tę technologię tak, aby nie była podatna na hakerskie włamanie.

W jaki sposób Google planuje wzmocnienie oprogramowania układowego?

„W ciągu ostatniej dekady pojawiło się wiele publikacji artykułów zwycięzców konkursu Pwn2Own i CVE o tematyce związanej z wykorzystaniem luk w oprogramowaniu układowym działającym w tych drugorzędnych procesorach” – czytamy w oświadczeniu Google. – „Błędy, które można wykorzystać zdalnie bezprzewodowo (np. błędy Wi-Fi i komórkowego pasma podstawowego) budzą szczególne obawy i dlatego

Google planuje wzmocnienie oprogramowania układowego w celu zwiększenia bezpieczeństwa ekosystemu Androida

**Bitdefender®**

są popularnym tematem podczas debat wśród społeczności badaczy bezpieczeństwa”.

Firma Google twierdzi, że opiera się na wcześniejszych osiągnięciach, takich jak wzmocnienie AP Androida poprzez umożliwienie łagodzenia skutków incydentów opartych na kompilatorze. Strategie te mają na celu „utrudnienie tworzenia powtarzalnych exploitów”, jednocześnie zapobiegając „przekształcaniu się niektórych typów błędów w luki w zabezpieczeniach”.

Google wspomniał także, że współpracuje z partnerami ekosystemu Androida w celu poprawy bezpieczeństwa oprogramowania układowego Androida, koncentrując się na odpowiednich mechanizmach ochrony, w tym:

- Eksploracji i aktywacji sanitizera opartego na kompilatorze (IntSan, BoundSan); komponenty te mogą wykrywać luki w zabezpieczeniach pamięci podczas kompilacji kodu.
- Mechanizmach łagodzenia exploitów, w tym integralności przepływu kontroli (CFI), integralności przepływu kontroli jądra (kCFI), ShadowCallStack i Stack Canaries.
- Włączanie funkcji bezpieczeństwa pamięci, takich jak automatyczne inicjowanie pamięci w oprogramowaniu układowym, aby zapobiec błędom krytycznym.

Google zdaje sobie sprawę, że zastosowanie mechanizmów łagodzenia

Google planuje wzmocnienie oprogramowania układowego w celu zwiększenia bezpieczeństwa ekosystemu Androida

**Bitdefender®**

exploitów w urządzeniach z Androidem może wpłynąć na ich wydajność, ale podkreśla znaczenie optymalizacji. Mówi się, że celem jest „maksymalizacja ochrony przy jednoczesnej minimalizacji wpływu na wydajność”.

Google już teraz jest w trakcie pracy mającej na celu zwiększenie bezpieczeństwa platformy Android. Niedawno firma ogłosiła, że jej wyczekiwany system operacyjny Android 14 będzie zawierał szereg nowatorskich technologii blokujących złośliwe oprogramowanie.

„Oprogramowanie Android ze względu na swoją otwartą architekturę jest szczególnie narażone na wszelkiego rodzaju włamania i cyberataki. Informacje o nieustannych pracach Google nad wzmocnieniem swojego produktu są istotne dla całej branży antywirusowej, ponieważ działania te pozytywnie wpłyną na ogólne podniesienie poziomu bezpieczeństwa użytkowników smartfonów. Nie możemy jednak zapominać o tym, że tylko skuteczny antywirus wyposażony w moduł antyphishingowy może ochronić nas przed większością zagrożeń związanych z korzystaniem z telefonu” – mówi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Źródło: <https://bitdefender.pl/google-planuje-wzmocnienie-oprogramowania-ukladowego-w-celu-zwiekszenia-bezpieczenstwa-ekosystemu-androida/>

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy

Google planuje wzmocnienie oprogramowania  
układowego w celu zwiększenia bezpieczeństwa  
ekosystemu Androida

**Bitdefender®**

Marken Systemy Antywirusowe jako źródła.

Data udostępnienia: 23.02.2023

Z pozdrowieniami Piotr Rozmiarek

E-mail: piotr.r@marken.com.pl | Tel. bezpośredni: 570 400 019

#### Informacje o firmie Bitdefender

Bitdefender to rumuński dostawca rozwiązań z zakresu cyberbezpieczeństwa oraz światowy lider chroniący miliony użytkowników. Bitdefender jest częstym zdobywcą wielu branżowych nagród i uznaną światową marką. Od 2001 roku konsekwentnie dostarcza najwyższej jakości produkty służące do zapewnienia bezpieczeństwa zarówno użytkownikom domowym, jak i wielkim korporacjom i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz wyposażania swojego oprogramowania w najnowsze technologie, takie jak uczenie maszynowe, heurystyka oraz EDR i XDR.

Google planuje wzmocnienie oprogramowania  
układowego w celu zwiększenia bezpieczeństwa  
ekosystemu Androida

**Bitdefender**<sup>®</sup>