Gli smartwatch per bambini venduti su Amazon sono facili da hackerare



I ricercatori di **Rapid7 Inc**., società di sicurezza informatica con sede a Boston, hanno scoperto delle vulnerabilità negli smartwatch per bambini venduti su Amazon.

Secondo la società, gli orologi intelligenti di fascia medio bassa, che vanno dai 20 a 35 dollari, hanno difetti critici che potrebbero consentire agli estranei di tracciare e parlare con chi li indossa.

Gli smartwatch testati da Rapid7 sono stati **Jsbaby Game Smart Watch** e Smartwatch per bambini **SmarTurtle**, tutti realizzati dalla società cinese **3G Electronics.** Rapid7 ha testato solo

tre dell’ampia varietà di smartwatch per bambini economici venduti su Amazon, quindi è possibile che altri modelli contengano gli stessi difetti.

“*È possibile che un utente malintenzionato con conoscenza del numero di telefono dello smartwatch possa assumere il controllo totale del dispositivo e quindi utilizzare la funzionalità di tracciamento e chat vocale con le stesse autorizzazioni dell’utente legittimo (in genere un genitore)*“, ha dichiarato a **Bloomberg Tod Beardsley**, direttore della ricerca di Rapid7.

Le problematiche degli smartwatch

Questi smartwatch sono dotati di funzioni GPS e di chat vocale, e i loro prezzi bassi, le funzionalità limitate e la facilità d’uso rispetto agli smartphone li rendono molto popolari per i genitori che vogliono sapere dove si trovano i loro figli o comunicare con loro senza smartphone.

Nonostante ciò Rapid7 ha affermato che questa misura di sicurezza, una whitelist, era un “controllo debole, anche nelle migliori circostanze”.

Un modo in cui un tutore può modificare le impostazioni dello smartwatch di un bambino da remoto è l’invio di un messaggio di testo al dispositivo. Ma per impedire agli estranei di modificare le impostazioni, è possibile creare un elenco di determinati numeri pre-approvati. Ma Rapid7 ha affermato che questa misura di sicurezza, una whitelist, era un “*controllo debole, anche nelle migliori circostanze*“.

La società di Boston ha scoperto che la whitelist non aveva alcun effetto su chi potesse modificare le impostazioni dello smartwatch. Chiunque, anche quelli che non erano nell’elenco pre-approvato, potrebbe inviare un messaggio di testo a uno di questi smartwatch per modificare le proprie impostazioni.

“*In pratica, questo filtro non sembrava affatto funzionale*“, ha dichiarato Beardsley.

L’altro difetto include le password predefinite dello smartwatch “12345” impostata per tutti i dispositivi. Rapid7 ha scoperto che i manuali dello smartwatch avevano poche o nessuna informazione sulle password predefinite e su come modificarle. A causa di questo ostacolo, è improbabile che gli utenti cambino la password predefinita, il che rende facile a chiunque l’accesso agli smartphone per ottenerne il controllo

Impossibile rintracciare i produttori

Questo problema di sicurezza potrebbe essere risolto con un aggiornamento del firmware adottato dal fornitore, ma “*è improbabile che un tale aggiornamento si materializzi dato che i fornitori di questi dispositivi sono difficili o impossibili da individuare*“, ha aggiunto la società di sicurezza informatica.

Rapid7 ha dichiarato che i suoi ricercatori non sono stati in grado di contattare nè i venditori né quello che credono sia il produttore degli orologi intelligenti, una società cinese chiamata **3g Electronics Co.**

Il consiglio di Rapid7 è di attenersi solamente a “*venditori chiaramente identificabili*“. In sostanza, se riconoscete questo marchio, statene alla larga.

https://www.key4biz.it/gli-smartwatch-per-bambini-venduti-su-amazon-sono-facili-da-hackerare/282462/