Achtung, Uhr hört mit

GPS-Tracking-Uhr lässt sich als Wanze missbrauchen

Tracking-Uhren sollen am Handgelenk von Kindern, Lebenspartnern oder Senioren für mehr Sicherheit sorgen. Bei einem Modell entdeckte ein Sicherheitsforscher in Zusammenarbeit mit c't jedoch eine Sicherheitslücke, mit der beliebige Träger von außen belauscht und getrackt werden können.

Von Fabian A. Scherschel

Als ein Bericht über Sicherheitslücken in Smartwatches einer kleinen österreichischen Firma per Mail in der Redaktion eintrudelte, klang die Beschreibung übertrieben und kaum zu glauben. Als uns unser Kontakt allerdings auf Nachfrage die Details der von ihm entdeckten Schwachstellen präsentierte, wurde schnell deutlich: der Sicherheitsforscher hatte nicht übertrieben. Die von ihm untersuchten Smartwatch-GPS-Tracker der Firma Vidimensio waren kinderleicht abzuhören. Mit einem einfachen Trick konnte man jede Uhr einer bestimmten Modellreihe dazu bringen, eine beliebige Telefonnummer anzurufen, ohne dass der Träger merkt, dass er abgehört wird – und das war nur eine von mehreren Angriffsmöglichkeiten.

Was diese Geschichte aber noch bemerkenswerter macht: Dieser Sicherheits-Alptraum hält bis heute an. Die Sicherheitslücken sind – bis zum Redaktionsschluss – nach wie vor vorhanden.

Abhörfunktionen verboten

Entdeckt hat die Lücken der unabhängige Sicherheitsforscher Christopher Dreher. Mit der Suche nach Schwachstellen von GPS-Tracking-Smartwatches hatte er begonnen, nachdem die Bundesnetzagentur im November 2017 gegen „Kinderuhren mit Abhörfunktion" vorgegangen war. In einer Stellungnahme warnte die Behörde damals vor Smartwatches, die Eltern dazu nutzen können, die Umgebung ihres Kindes abzuhören. Eltern hatten diese etwa dazu verwendet, Lehrer im Unterricht zu belauschen. Geräte mit solchen Funktionen sind laut der Bundesnetzagentur in Deutschland verboten und müssen zerstört werden. Eltern wird sogar geraten, Nachweise über die Vernichtung der Geräte aufzubewahren. Das deutet bereits an, wie ernst die Behörde solche Funktionen nimmt.

Dreher entdeckte beim Onlineversand Amazon eine Smartwatch namens Paladin des Herstellers Vidimensio, der auf seiner Webseite GPS-Tracker zum Schutz von Kindern, Senioren, Haustieren und Fahrzeugen bewirbt. Bei Amazon hatte die Firma das Produkt explizit mit den Worten „ohne Abhörfunktion" angepriesen. Das weckte den Ehrgeiz des auf Pentesting spezialisierten Sicherheitsforschers.

Nachdem er die Uhr auf seinem Schreibtisch hatte, musste Dreher nicht lange nach Lücken suchen. Die Uhr Paladin wird mit Hilfe einer Android- oder iOS-App konfiguriert, da das Gerät selbst nur eine sehr rudimentäre Benutzeroberfläche besitzt. Die App kommuniziert mit einem Webserver des Herstellers, der wiederum Befehle an die Uhr über eine Mobilfunkverbindung schickt. Zu Drehers Erstaunen war der Datenverkehr zwischen App und Server komplett unverschlüsselt.

So konnte der Sicherheitsforscher nicht nur herausfinden, unter welcher Adresse der Server des Herstellers im Netz zu erreichen ist, sondern auch, welche Befehle er genau entgegennimmt. Er konnte das Passwort des Vidimensio-Kon-

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover

tos seiner Uhr und deren interne, einzigartige ID-Nummer auslesen.

Mit dem Passwort hätte sich jeder, der es etwa in einem öffentlichen WLAN aufschnappt, über die Vidimensio-Server anmelden und Drehers Uhr verwalten können. So hätte der Angreifer zum Beispiel die auf der Uhr gespeicherten Kontaktdaten und deren GPS-Position in Echtzeit auslesen können. Das alleine wäre schon eine schwerwiegende Sicherheitslücke gewesen.

Doch es kommt noch viel schlimmer: Der Sicherheitsforscher entdeckte, dass eine Anmeldung auf dem Server gar nicht nötig ist. Allein die ID einer Uhr genügte, um dieser über den Hersteller-Server Befehle zu schicken. Da die IDs offensichtlich nicht zufällig vergeben werden, sondern mit jeder neuen Uhr hochzählen, hätte der Forscher auch auf beliebige andere Paladin-Uhren zugreifen können.

Totale Kontrolle

Angriffe auf die Uhren hätten einfacher nicht sein können: Die Befehle an die Uhr schickt man mit einem einfachen POST-Request, wie man ihn etwa mit Linux-Kommandozeilenprogrammen wie wget oder curl absetzen kann. Man kann die Position der Uhr auslesen, ihr ein neues Passwort zuweisen oder die Konfiguration zurücksetzen.

Im weiteren Verlauf seiner Untersuchung entdeckte Dreher dann noch eine undokumentierte Funktion der Uhr, die es in sich hat: Damit kann man die Uhren, die bei Amazon explizit als „ohne Abhörfunktion“ beworben wurden, in eine Wanze verwandeln. Schickt man der Uhr über den Hersteller-Server eine Telefonnummer, ruft diese daraufhin die Nummer an und der Empfänger kann alles hören, was im Umfeld der Uhr gesagt wird. Der Träger der Uhr bekommt davon nichts mit. In der Benutzeroberfläche gibt es nicht das geringste Anzeichen dafür, dass der Anruf stattfindet oder das Mikrofon der Uhr in Benutzung ist. Genau vor dieser Art verdeckter Spionage hatte die Bundesnetzagentur in ihrer Pressemitteilung ausdrücklich gewarnt.

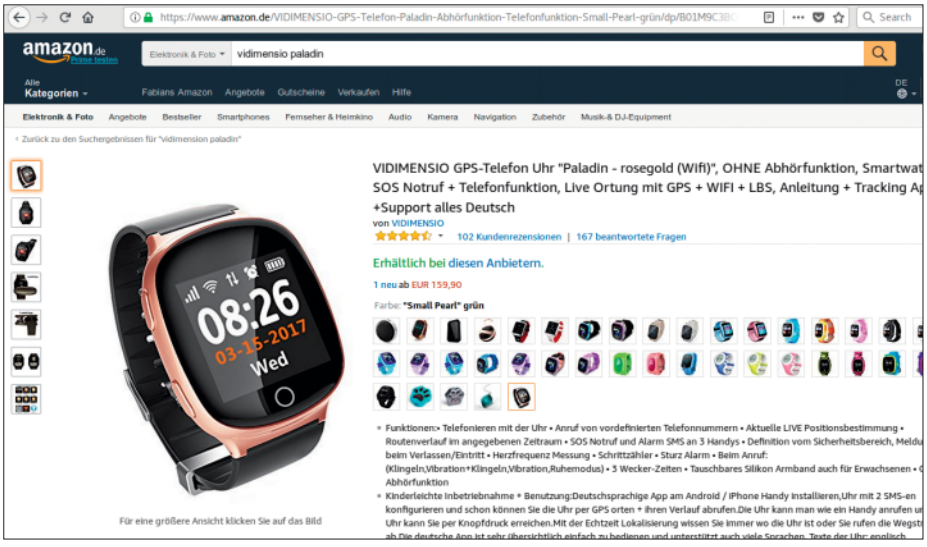
Mit der nicht dokumentierten Funktion der Uhr kann man diese aber nicht nur abhören. Denkbar wäre auch, fremde Uhren dazu zu bringen, gebührenpflichtige Nummern anzurufen. Unsere Tests legen nahe, dass Vidimensio hunderte Uhren verkauft hat. Ein Angreifer könnte die Lücken mit geringem Aufwand automatisch ausnutzen, um den Besitzern unbemerkt per Premium-Nummer Geld aus der Tasche zu ziehen. c't konnte diese Sicherheitslücken anhand einer von uns für diesen Zweck gekauften Paladin bestätigen.

Kein Einsehen beim Hersteller

Auf Grund der Brisanz seiner Erkenntnisse wandte sich Dreher an die Redaktion von heise online und c't: Wir sollten die Kommunikation mit dem Hersteller übernehmen und so dafür sorgen, dass die Schwachstellen geschlossen werden, bevor die Öffentlichkeit von ihnen erfährt. Das ist uns auch fast drei Monate nach unserer ersten Kontaktaufnahme mit dem Hersteller nicht gelungen.

Unser Kontakt bei Vidimensio, allen Anzeichen nach eine Limited mit Sitz in Birmingham, die in erster Linie über eine Zweitniederlassung in Wien zu erreichen ist, tauschte zwar fleißig E-Mails mit uns aus. Er wollte aber offensichtlich nicht einsehen, wie brisant die von Dreher entdeckten Lücken in den Uhren sind. Statt uns mitzuteilen, bis wann er die Lücken schließen könnte, diskutierte der Firmenchef mit uns darüber, ob die Geschichte eine Veröffentlichung rechtfertige. Seiner Ansicht nach war seine Firma viel zu klein und seine Produkte viel zu unbedeutend, als dass wir sie mit einem Artikel beehren sollten. Es gebe doch viele andere, viel wichtigere Sicherheitslücken, über die wir lieber berichten sollten.

Dass die Käufer seiner Uhren erfahren sollten, dass sie mit Wanzen am Handgelenk herumlaufen, auf die jedermann aus dem Internet nach Belieben zugreifen kann, wollte der Firmenchef nicht einsehen. Auf mehrfache Bitten, uns einen Termin zu nennen, wann er die ihm seit Anfang Januar bekannten Sicherheitslücken stopfen könne, erhielten wir bis heute keine für uns befriedigende Antwort. Als wir den Vidimensio-Chef um Stellungnahme zu den von Dreher entdeckten Lücken baten, antwortete er uns, man habe die Sicherheitslücken mit einem Update der Android- und iOS-Apps behoben. Außerdem bezeichnet er das Modell Paladin als „eine nicht besonders beliebte Uhr“. Man habe nur „eine sehr



Stimmt nicht: Der Hersteller weist in seinem Amazon-Angebot deutlich darauf hin, dass die Uhr keine Abhörfunktion besitzt.

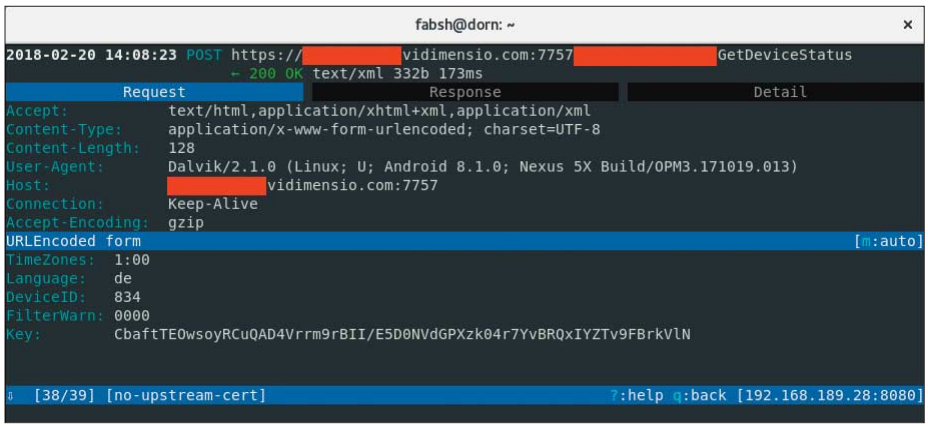
heise Investigativ

Viele der c't-Investigativ-Recherchen sind nur möglich dank Informationen, die Leser und Hinweisgeber direkt oder anonym an uns übermitteln.

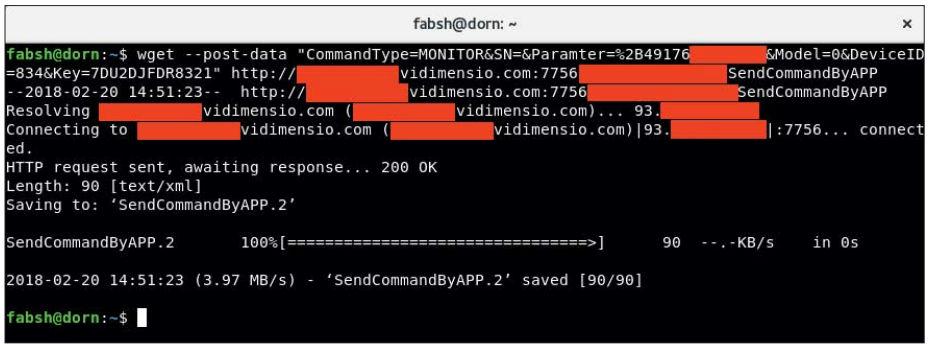
Wenn Sie selbst Kenntnis von einem Missstand haben, von dem die Öffentlichkeit erfahren sollte, können Sie uns einen anonymen Hinweis oder brisantes Material zukommen lassen. Nutzen Sie dafür bitte unseren anonymen und sicheren Briefkasten.

https://heise.de/investigativ

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover



Selbst nach dem Update der Vidimensio-App lässt sich aus deren Traffic die Device ID der Zieluhr (DeviceID) auslesen. Unsere Uhr ist Nummer 834.



Mit diesem Linux-Einzeiler funktionieren wir unsere Uhr in eine Wanze um, ohne dass wir dafür ein Passwort benötigen.

geringe Stückzahl" nach Deutschland verkauft. Auf die Mitteilung der Bundesnetzagentur im November habe man „sofort reagiert". „Die Abhörfunktion bei der Uhr Paladin, wie auch bei anderen Uhren" sei mit dem App-Update aus dem Februar abgeschaltet worden. Unsere Tests im März belegen jedoch, dass dies nicht stimmt.

Nicht nur wir kommunizierten mit der Firma. Nachdem der Entwickler der Vidimensio-Software unseren Informanten Dreher als Sicherheitsforscher identifiziert hatte, kontaktierte er ihn direkt. Der Vidimensio-Chef hatte ihn, so Drehers Vermutung, anscheinend beim Kauf seiner Test-Uhr über die Endung seiner Mailadresse als Sicherheitsforscher identifiziert. In der resultierenden Mail-Konversation versuchte der Sicherheitsforscher, wie er uns berichtete, die Firma ebenfalls dazu zu bringen, die Probleme mit ihrem Produkt ernst zu nehmen.

Richtig ist: Im Laufe unserer Tests spielte Vidimensio ein Software-Update für die Android- und iOS-Apps aus. Nach diesem Update im Februar wurde der Datenverkehr zwischen App und Server TLS-verschlüsselt. Vidimensio hatte diese Änderung auf Anraten Drehers vorgenommen. Sie ist allerdings nur ein Tropfen auf den heißen Stein. Da die App auch nach diesem Update kein Zertifikats-Pinning vornimmt, ist es mit Werkzeugen wie etwa der Software mitmproxy trivial einfach, ein eigenes TLS-Zertifikat auf einem Handy mit Vidimensio-App zu installieren und den Datenverkehr trotzdem auszulesen.

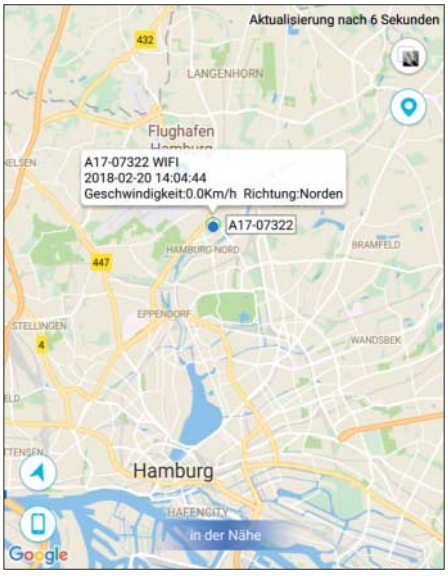
Das Update verhindert zwar Angriffe auf die App in öffentlichen WLAN-Hotspots, für einen Sicherheitsforscher, der seine eigene Uhr analysieren will, stellt der zusätzliche Schutz allerdings nur eine kleine Unannehmlichkeit dar. Und: Auch der Angriffsweg über wget blieb offen. Wer einmal die Zusammensetzung der ausführbaren Server-Anweisungen kennt, kann auch ganz ohne App-Analyse die Abhörfunktion aktivieren.

Dreher unternahm mehrere Versuche, den Hersteller davon zu überzeugen, dass die TLS-Verschlüsselung der App nur ein erster Schritt zur Absicherung der Uhren sei. Der Hersteller müsse das öffentlich erreichbare Server-API wenigstens mit einer Anmelde-Routine absichern. Besser noch wäre natürlich belastbare Ende-zu-Ende-Verschlüsselung zwischen Uhren und Apps auf der einen und dem Server auf der anderen Seite gewesen. Allerdings gab auch Dreher nach mehreren Wochen der Diskussion auf und berichtete uns, er habe noch es nie mit einem uneinsichtigeren Hersteller zu tun gehabt.

Die Uhren gehören aus dem Verkehr gezogen

Bei Redaktionsschluss war es uns nach wie vor möglich, allein unter Angabe der ID Befehle an eine Uhr zu schicken und diese abzuhören. Das entspricht unserer Einschätzung nach der Abhörfunktion genau jener Uhren, gegen die die Bundesnetzagentur Ende 2017 vorgegangen ist und die damals zerstört werden mussten.

Eine eingehende Analyse der Server-Infrastruktur legt den Verdacht nahe, dass andere Produkte der Firma Vidimensio ähnliche Sicherheitslücken enthalten. Nach Angaben der Firma verwenden alle von ihr vertriebenen GPS-Uhren dieselbe App, was darauf hindeuten würde, dass sie ebenfalls über dieselben Server verwaltet werden. Der Hersteller teilte uns dazu pauschal mit, dass mit dem Februar-App-Update alle Lücken geschlossen seien und „die Abhörfunktion bei der Uhr Paladin wie auch bei anderen Uhren von uns abgeschaltet" wurde. *(fab@ct.de)* c't



Über die Vidimensio-App lässt sich die Position jeder Uhr in Echtzeit auslesen. Wenn man weiß wie, stellt der Server die Rohdaten aller Uhren auch bereit, ohne dass man sich einloggen muss.

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover