



Brief

Key Personnel Security Risks of Fitness Trackers

B-2023-06-28a

Classification: TLP:CLEAR

Criticality: High

Intelligence Requirements: Personal Disclosures, Residential, Travel

June 28, 2023

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 3:00 PM (EDT) on June 27, 2023**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | Key Personnel Security Risks of Fitness Trackers

Executive Summary

A recent report of exposure risks in fitness trackers serves as a reminder of the potential safety hazards these trackers can pose. Fitness trackers are extremely popular; they help users track their fitness activity, share results on social media, and connect with other fitness enthusiasts. Fitness tracker risks are not new; there have been several well-documented vulnerabilities associated with utilizing them over the past few years. These vulnerabilities have included several instances in which using fitness trackers has led to inadvertent disclosures of key personnel locations, whether it be military personnel or executives. In this brief, ZeroFox reviews the recent concerns, overall potential risks, and recommendations for limiting risk and exposure for key personnel.

Details

Security researchers at North Carolina State University Raleigh have uncovered a privacy risk in fitness app Strava's heat map feature, which aggregates activity data to help users find exercise spots. The researchers were able to achieve a 37.5 percent accuracy rate in predicting users' home locations using publicly available data.¹ The publicly available data was overlaid with the user start/stop locations and routes and then correlated back to the specific users. These findings are reminiscent of previous fitness

¹ <https://news.ncsu.edu/2023/06/fitness-app-privacy-loop-hole/>

tracker risks that displayed the whereabouts of non-public U.S. military stations and tracked movements to and from sensitive locations, such as the White House.²³

Analyst Commentary

Disclosures through these fitness trackers can open key personnel to several security risks. When the routes they frequent are publicly available, a potential threat actor could correlate these maps with residences and regularly-traversed routes and use them to stalk the victim. As seen with the most recent vulnerability, tracking start/stop locations and overlaying that with street views exposes residential information.⁴ Threat actors can utilize common data aggregators to then correlate that back to specific people. This can put key personnel such as military leaders or executives, their families, and their associated organizations at an increased risk for targeting. The recommendations section below outlines some practical ways to limit these exposures.

In addition to possible disclosures that can be gleaned from the app itself, users' self-disclosures can also present serious risks—such as opening them up to stalking risks and threat actor targeting. Self-disclosures have the potential to be viewed by users' social media connections. Depending on their social media platform settings, users' posts may be publicly accessible or viewable by connections of their connections, making them more susceptible to targeting—particularly if they frequent the same routes or follow a similar fitness routine regularly.

Further, data shared from fitness tracker apps can potentially disclose information to third parties. Because the data collected by fitness trackers is not considered to be health information, it does not have the same mandated protections that health-related

2

[hXXps://www.engadget\[.\]com/2018-03-13-after-exposing-secret-military-bases-strava-restricts-data-visi.html](https://www.engadget.com/2018-03-13-after-exposing-secret-military-bases-strava-restricts-data-visi.html)

3

[hXXps://www.vice\[.\]com/en/article/v7b4zy/alltrails-data-exposes-precise-movements-of-former-top-biden-official](https://www.vice.com/en/article/v7b4zy/alltrails-data-exposes-precise-movements-of-former-top-biden-official)

4

[hXXps://www.bleepingcomputer\[.\]com/news/security/strava-heatmap-feature-can-be-abused-to-find-home-addresses/](https://www.bleepingcomputer.com/news/security/strava-heatmap-feature-can-be-abused-to-find-home-addresses/)

apps do.⁵ However, fitness trackers have access to location, fitness, and other personal information that could then be shared with third parties, which could also be utilized to target key personnel if breached or otherwise end up in threat actor possession.

Recommendations

While it is unlikely that key personnel will discontinue the use of fitness apps altogether, below are some recommendations to manage their exposure when utilizing these apps:

- Key personnel should be made aware of the potential for disclosures on fitness tracker apps and the risks that accompany these disclosures (both from self-disclosures and disclosures from the apps).
- Advise key personnel to limit the location-sharing permissions on their mobile and smart devices; if they must use location sharing, enabling the feature after they are some distance away from their homes will limit the start/stop correlation to their residences.
- Anonymize usernames and refrain from uploading personal photos.
- Opt out of contributing data to the “aggregated data usage” feature in fitness trackers.
- Ensure that the privacy settings for social media accounts are as stringent as possible to limit the reach of self-disclosures.
- Review the app’s policies on data-sharing with third parties, understand what data may be shared, and opt out to the greatest extent possible.
- Engage with the ZeroFox Protection Intelligence Team to conduct a comprehensive Executive Threat Assessment on company executives at least once per year. You can request an Executive Threat Assessment via the [RFI button](#) in the ZeroFox platform.
- Leverage ZeroFox’s Personally Identifiable Information (PII) Removal services to keep your executive and key personnel’s PII secure, and remove their PII from data broker sites and Google searches.
- Leverage ZeroFox’s [Physical Security Intelligence](#) solution for continuous monitoring of digital threats to the physical safety of key personnel, their homes, offices, and travel locations.

⁵ <https://www.cnbc.com/2022/11/26/the-biggest-risks-of-using-fitness-trackers-to-monitor-health.html>

| Appendix: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.