WhisperPair

Hijacking Bluetooth Accessories Using Google Fast Pair

Is my device vulnerable?

About | Cite | Watch the video

Bluetooth hijacking

Many Bluetooth accessories do not implement Google Fast Pair correctly, enabling an attacker to forcefully pair with a vulnerable accessory.

Learn more

Location tracking

If an accessory has never been paired with an Android device, an attacker may be able to track its location using Google's Find Hub Network.

Learn more

Cross-ecosystem impact

Since the Fast Pair functionality of an accessory cannot be disabled, users outside the Android ecosystem are also vulnerable to WhisperPair.

Learn more

About

Google Fast Pair enables one-tap pairing and account synchronisation across supported Bluetooth accessories. While Fast Pair has been adopted by many popular consumer brands, we discovered that many flagship products have not implemented Fast Pair correctly, introducing a flaw that allows an attacker to hijack devices and track victims using Google's Find Hub network.

We introduce *WhisperPair*, a family of practical attacks that leverages a flaw in the Fast Pair implementation on flagship audio accessories. Our findings show how a small usability 'add-on' can introduce large-scale security and privacy risks for hundreds of millions of users.

Hijacking Fast Pair Accessories

WhisperPair enables attackers to forcibly pair a vulnerable Fast Pair accessory (e.g., wireless headphones or earbuds) with an attacker-controlled device (e.g., a laptop) without user consent. This gives an attacker complete control over the accessory, allowing them to play audio at high volumes or record conversations using the microphone. This attack succeeds within seconds (a median of 10 seconds) at realistic ranges (tested up to 14 metres) and does not require physical access to the vulnerable device.

The flaw stems from many accessories failing to enforce a critical step in the pairing process. To start the Fast Pair procedure, a *Seeker* (a phone) sends a message to the *Provider* (an accessory) indicating that it wants to pair. The Fast Pair specification states that if the accessory is not in pairing mode, it should disregard such messages. However, many devices fail to enforce this check in practice, allowing unauthorised devices to start the pairing process. After receiving a reply from the vulnerable device, an attacker can finish the Fast Pair procedure by establishing a regular Bluetooth pairing.

Tracking Victims Using Google's Find Hub Network

Some devices also support Google's Find Hub network. This enables users to find their lost accessories using crowdsourced location reports from other Android devices. However, if an accessory has never been paired with an Android device, an attacker can add the accessory using their own Google account. This allows the attacker to track the user via the compromised accessory. The victim may see an unwanted tracking notification after several hours or days, but this notification will show their own device. This may lead users to dismiss the warning as a bug, enabling an attacker to keep tracking the victim for an extended period.

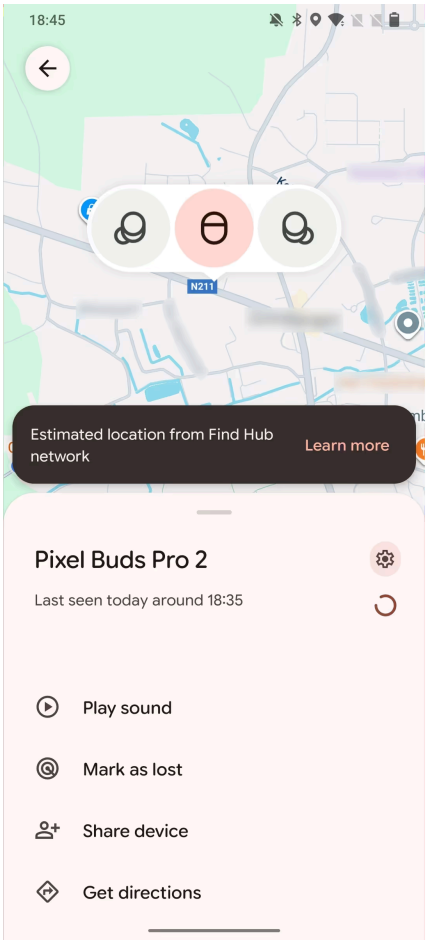

Figure 1: Attacker's dashboard with location from the Find Hub network.

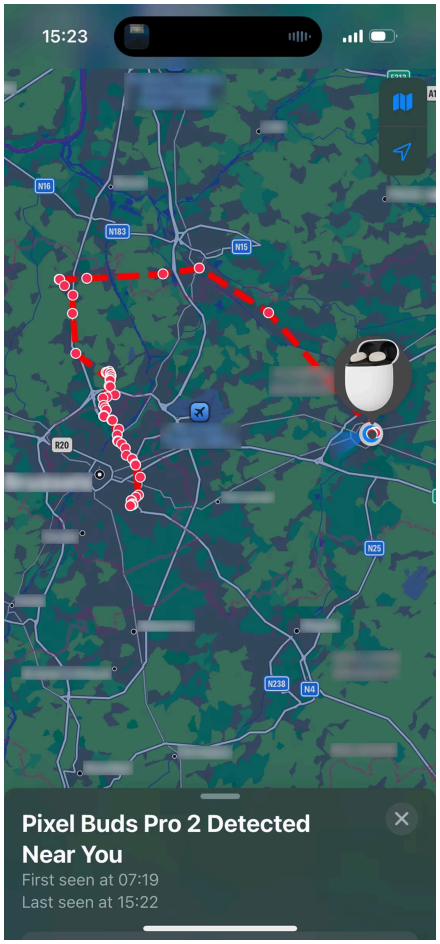

Figure 2: Unwanted tracking notification showing the victim's own device.

This attack exploits the fact that non-Android devices do not perform the Fast Pair procedure when they connect to an accessory. Android devices write an *Account Key* to the accessory after the pairing has completed. This key is used to establish ownership of the device, as the first key written to a device is marked as the *Owner Account Key*. Therefore, if the victim has never connected their accessory to an Android device, the attacker will be marked as the owner after writing their account key.

Impact

WhisperPair is not an isolated issue. Our study shows that multiple devices, vendors, and chipsets are affected. These vulnerable devices passed both the manufacturers' quality assurance tests and Google's certification process, demonstrating a systemic failure rather than an individual developer error. While there is a certification process that devices must undergo before the Fast Pair functionality is activated, insecure implementations still reached the market at scale. This shows a chain of compliance failures in Google Fast Pair, as the vulnerability failed to be detected on all three levels: implementation, validation, and certification.

The consequences of WhisperPair are severe, allowing an attacker to pair with a vulnerable device in seconds. The attack can be performed using commodity hardware and does not require user interaction. In some scenarios, an attacker may also be able to add the accessory to the Find Hub Network using a malicious account.

Responsible disclosure & mitigation

We reported our findings to Google in August 2025, who classified the issue as critical (CVE-2025-36911). We agreed on a 150-day disclosure window, during which Google could work with their ecosystem partners to release security patches. Google awarded us the maximum possible bounty of $15,000 for this issue. We would like to thank the Android Security Team for their responsiveness and collaboration throughout the disclosure process.

The only way to fix this vulnerability is by installing a software update issued by the manufacturer of the accessory. Although many manufacturers have released patches for their impacted devices, software updates may not yet be available for every vulnerable device. We encourage researchers and users to verify patch availability directly with the manufacturer.

Questions and Answers

Who conducted this research?

Is my device vulnerable?

How can I protect myself against this attack?

Can a vulnerability like WhisperPair be prevented in the future?

If I have an iPhone, does that mean I am not vulnerable?

I updated my phone. Am I safe now?

Does unpairing or factory resetting fix the issue?

Can I turn off Google Fast Pair?

Where can I find more information?

Does an attacker need special hardware to perform the attack?

Media Coverage (selection)

English

- WIRED, "Hundreds of Millions of Audio Devices Need a Patch to Prevent Wireless Hacking and Tracking" by Andy Greenberg and Lily Hay Newman
- 9to5Google, "Many Google Fast Pair devices need an update to patch exploits that allowed attackers to track you" by Will Sattelberg
- BleepingComputer, "Critical WhisperPair flaw lets hackers track, eavesdrop via Bluetooth audio devices" by Sergiu Gatlan
- Android Authority, "Update your headphones: Fast Pair vulnerability could let attackers track your location" by Taylor Kerns
- Android Police, "Google Fast Pair devices need an immediate update for hacking risk" by Matthew Mountjoy
- Macworld, "This strange Google Fast Pair flaw even puts users with iPhones at risk" by Jason Cross
- Engadget, "Flaw in 17 Google Fast Pair audio devices could let hackers eavesdrop" by Will Shanklin
- Ars Technica, "Many Bluetooth devices with Google Fast Pair vulnerable to “WhisperPair” hack" by Ryan Whitwam
- SoundGuys, "Major security flaw affects Sony, Google, and other popular headphones" by Adam Birney
- Inc., "Google Says It Fixed a Bluetooth Flaw. Researchers Claim Hackers Can Still Track You" by Leila Sheridan
- Stuff, "Google Fast Pair security flaw allowed for easy eavesdropping on Android users" by Chris Smith
- Gizmodo, "You Need to Check Your Wireless Headphones for Updates, Right Now" by Ece Yildirim
- Cybernews, "Google Bluetooth flaw puts millions of audio devices at risk" by Stefanie Schappert
- ZDNET, "Check your earbuds ASAP for this flaw that lets attackers spy on you - here's how" by Charlie Osborne
- CyberInsider, "WhisperPair attack exposes millions of Bluetooth devices to location tracking" by Alex Lekander
- SecurityWeek, "WhisperPair Attack Leaves Millions of Audio Accessories Open to Hijacking" by Ionut Arghire
- The Verge, "Sony, Anker, and other headphones have a serious Google Fast Pair security vulnerability" by Andrew Liszewski
- The New York Times, "Wireless Earbuds Can Be Hacked. Here's How to Protect Yourself." by Max Eddy
- PC Gamer, "Audio devices that use Google's Fast Pair Bluetooth tech are vulnerable to hacks that could track location or listen to the mic, according to researchers" by Nick Evanson
- The Register, "Fast Pair, loose security: Bluetooth accessories open to silent hijack" by Carly Page
- Zee News, "Google Fast Pair Flaw: Earbuds, And Headphones At Risk Of Hacking And Tracking; Here's How To Stay Protected" by Ankur Mishra
- The Indian Express, "This is how hackers can hijack your earbuds to spy on you"
- Fox News, "Google Fast Pair flaw lets hackers hijack headphones" by Kurt Knutsson

Dutch

- De Morgen, "Beveiligingslek in Bluetooth-oortjes laat meeluisteren en volgen toe" by Joanie de Rijke
- Het Nieuwsblad, "Leuvense onderzoeker over 'kritiek' lek in beveiliging van Bluetooth: “Het grootste dat we ooit ontdekten”" by Arthur De Meyer
- Datanews, "Leuvense onderzoekers vinden lek in Bluetooth pairingdienst Google" by Els Bellens

- TechPulse, "Snelle bluetoothverbinding van Google maakt je kwetsbaar voor afluisterpraktijken" by Steven Kins
- Computable, "Bluetooth onder druk: Fast Pair blijkt achilleshiel voor privacy" by William Visterin
- Het Laatste Nieuws, "Ernstig beveiligingslek in Bluetooth-oortjes: ongemerkt meeluisteren én volgen mogelijk" by KVE
- Androidworld, "Let op: hackers kunnen je locatie tracken via je oordopjes" by Laura Jenny
- Bright, "Miljoenen oordopjes en koptelefoons zijn kwetsbaar: wie luistert er met je mee?" by Erwin Vogelaar

Other

- Le Soir (French), "Vos écouteurs Bluetooth peuvent vous espionner : la faille Google révélée par la KU Leuven" by Philippe Laloux
- Golem (German), "Sicherheitslücke macht Hörstöpsel zur Wanze" by Michael Linden
- Ultima Hora (Spanish), "Un fallo en Fast Pair expone millones de auriculares y altavoces a un secuestro" by Michael Linden
- Benchmark (Serbian), "Milioni slušalica i zvučnika izloženi hakovanju: Fast Pair Google propust omogućava prisluškivanje i praćenje" by Aleksandar Božović
- Clubic (French), "Sony, JBL, Google : pourquoi vous devez mettre à jour vos écouteurs Bluetooth de toute urgence" by Stéphane Ficca
- Computerworld (Danish), "Alvorlig Bluetooth-fejl rammer hundredvis af millioner: Hackere kan aflytte dine samtaler og spore din position" by Frederik Therkildsen
- Android.com.pl (Polish), "Zagrożenie dla słuchawek przez lukę. Natychmiast zaktualizuj oprogramowanie" by Jolanta Szczepaniak
- Bug (Croatian), "Ozbiljan sigurnosni propust u Googleovom Fast Pairu ugrožava vlasnike bežičnih slušalica"
- Euronews Turkey (Turkish), "Bluetooth kulaklık kullanıcılarına uyarı: Milyonlarca kişi izinsiz takip riski altında" by Cagla Uren
- RTS (Serbian), "Možda vas špijunira uređaj na glavi - Srbin deo tima koji je otkrio Guglov propust, iznosi detalje za RTS" by Goran Belanović
- Corriere della Sera (Italian), "I ricercatori hanno scoperto una falla negli auricolari Bluetooth che permette di localizzare l'utente e ascoltarne le conversazioni" by Roberto Cosentino
- Navbharat Times (Hindi), "14 □□□ □□□ □□ 15 □□□□□ □□□ '□□□□□□' □□ □□□□□ □□□□□□□ □□□□□□□, □□ □□□□ □□□□ □□ □□□□□□ □□ □□□□□□, □□□□□□ □□□ □□□□□□" by Mona Dixit
- adn (Mexican), "Fallo en Fast Pair expone audífonos Bluetooth a hackeo y rastreo" by Joy Uricare
- Tuổi Trẻ (Vietnamese), "Lỗ hổng nghiêm trọng trên Google Fast Pair: Tai nghe Bluetooth có thể thành thiết bị nghe lén" by Đông Hải

This work was supported by the Flemish Government through the Cybersecurity Research Program with grant number: VOEWICS02.