Security Assessment Report

Beat XP VEGA Smartwatch — BLE Denial of Service (Session Lock)

Device: Beat XP Vega
Firmware Version: RB303ATV006229

Report Date: 03/12/2025
Company Name: Beat XP
Contact Email: support@beatxp.com

Document History

Version	Date	Author	Remark
1.0	03/12/2025	Nikhil Yalgar	First Draft

1 Security Assessment Details

1.1 Executive Summary

A security assessment of the Beat XP VEGA Smartwatch (Firmware RB303ATV006229) focused on Bluetooth Low Energy (BLE) connectivity revealed a design and implementation weakness that enables a nearby BLE central device to establish and retain the single available BLE session without authentication or session access control. Because the smartwatch's BLE stack permits only one active connection at a time and lacks session preemption or authorization checks, a rogue central can monopolize the connection slot indefinitely. While connected, legitimate companion applications (e.g., the official mobile app) are unable to connect, resulting in a denial-of-service (DoS) condition for configuration, synchronization, and diagnostics. The issue arises from missing authentication/authorization at the BLE connection layer and inadequate session management policies. The assessment classified this finding as high severity and recommends prioritized remediation to prevent operational disruption.

1.2 Scope and Objectives

The assessment scope was limited to the Bluetooth Low Energy (BLE) interface and connection-handling logic of the Beat XP VEGA Smartwatch (Firmware RB303ATV006229). Objectives:

- Identify weaknesses in BLE connection acceptance, session control, and authentication.
- Evaluate the impact on availability and device management workflows.
- Provide recommendations to mitigate and remediate the identified issues.

1.3 Technology Impact Summary

Assessment of the device BLE interface identified that an unauthenticated nearby BLE central can establish a persistent session that blocks subsequent legitimate connection attempts, producing the following technical impact:

- Persistent resource lock of the BLE connection slot (single-connection limitation).
- Denial of synchronization, configuration, and firmware update operations that rely on BLE connectivity.

1.4 Business Impact Summary

- Customers may be unable to sync health data, apply configuration changes, or receive firmware updates while the device is locked by an unauthorized BLE client.
- Repeated or targeted misuse may lead to negative user experience, increased support costs, and reputational damage.

1.5 Testing Environment and Tools

Wireless testing was conducted using standard BLE tools and smartphone applications:

- Official companion app (BeatXP — used as representative legitimate app)
- nRF Connect (Android/iOS) for scanning and establishing BLE central connections
- Typical BLE-capable smartphones used as adversary centrals

1.6 Table of Findings

Finding ID	**Scope**	**Finding**	**CVSS Score**	**CVSS Vector**	**Severity**	**Status**
BXP-DoS-01	BLE	Denial of Service (DoS)	7.1	CVSS:4.0 / AV:A / AC:L / AT:N / PR:N / UI:N / VC:N / VI:N / VA:H / SC:N / SI:N / SA:N	High	Not Fixed

1.7 Device Strengths

Not assessed in this engagement (scope limited to BLE). No additional strengths were evaluated.

1.8 Device Weaknesses

- BLE connection-handling accepts unauthenticated centrals and enforces a single active connection without preemption or session-level authorization.

2 Technical Findings

2.1 BXP-DoS-01: Denial of Service

Potential Impact: High

Description

The Beat XP Vega smartwatch's BLE peripheral accepts incoming connections from any BLE-capable central device without performing authentication or bonding checks and supports only one active BLE connection at a time. An unauthenticated central can therefore establish and retain the sole active session. While this session is active, all new connection attempts (including from the official companion application) are rejected or fail to discover/connect, effectively rendering BLE-based management and synchronization features unavailable until the rogue session is terminated.

Affected Components

- BLE peripheral stack (connection acceptance logic)
- Session management and connection-handling firmware modules
- Companion application functionality that depends on BLE connectivity (sync, configuration, firmware update)

Technical Risk

The inability of legitimate centrals to connect causes loss of availability for BLE-dependent operations: data sync, configuration pushes, diagnostics, and OTA workflows (if reliant on BLE). This may prevent timely application of critical settings or updates.

Business Risk

End users may experience failed syncs, lost configuration changes, and inability to perform device maintenance operations. Recurring incidents could erode customer confidence and increase support/returns.

Mitigation

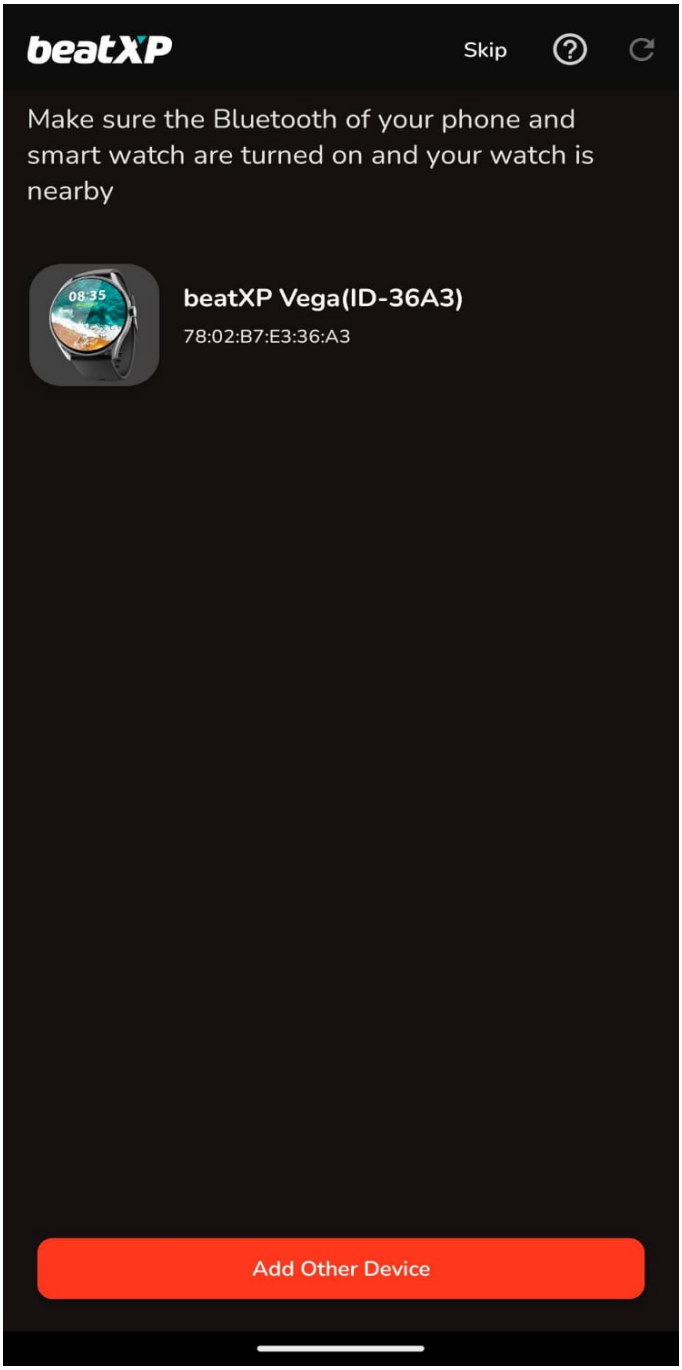
Primary mitigations:

- Restrict Access with Whitelisting or MAC Filtering: Only allow specific, trusted BLE central devices to establish connections, reducing the risk of rogue clients.
- Enforce BLE-Level Authentication and Encryption: Require secure pairing and bonding before allowing access to any critical services or configuration characteristics.

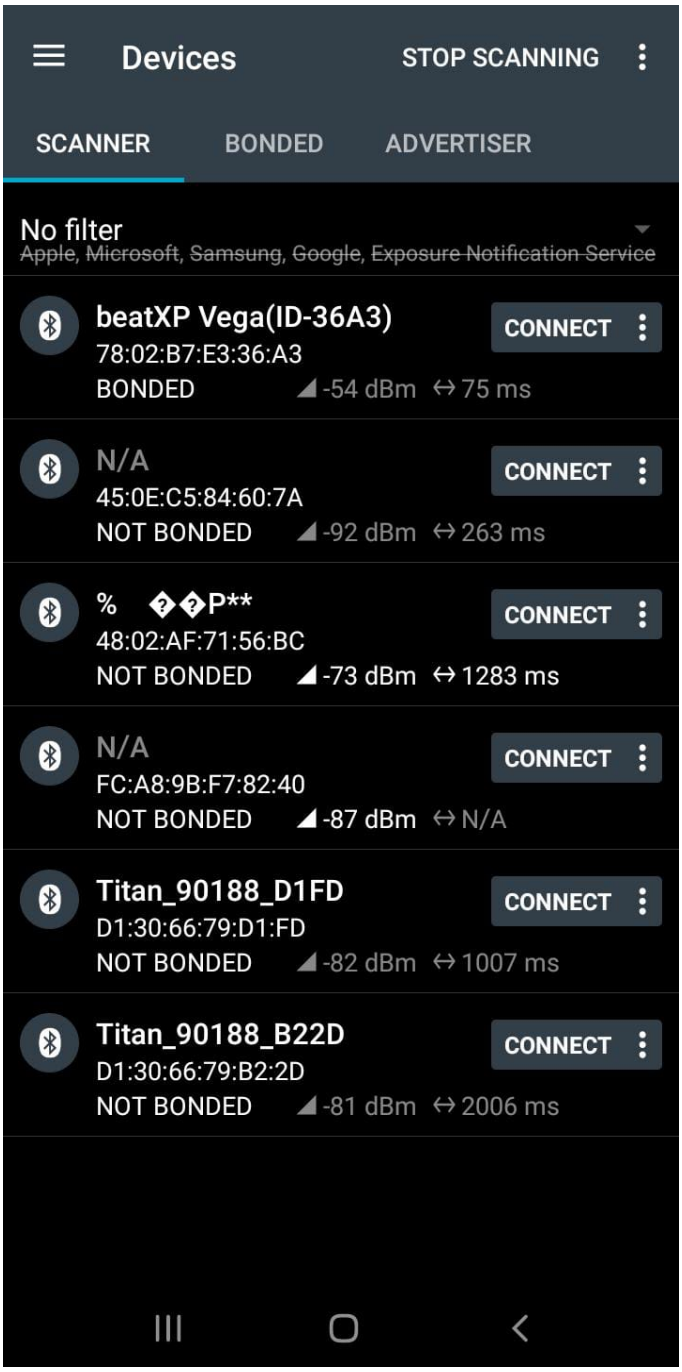
- Implement Application-Layer Session Control: Add logic to reject or disconnect non-compliant clients that do not perform valid operations (e.g., GATT read/write) within a defined timeframe, ensuring only legitimate configuration tools retain access.

Steps to Reproduce (Proof of Concept)

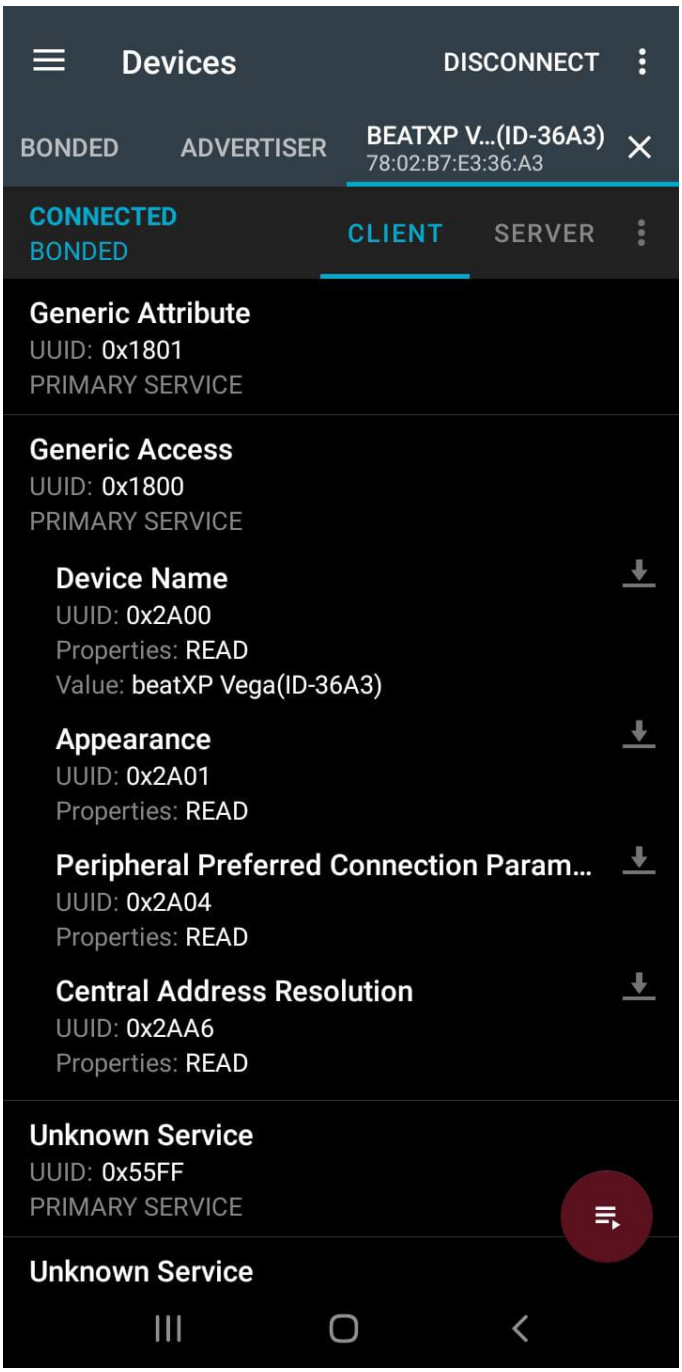
1. Ensure the Beat XP smartwatch (Firmware RB303ATV006229) is powered on and advertising BLE for companion connectivity
2. On a smartphone running the official companion app (e.g., BeatXP Fit), verify the watch is discovered and connectable.



3. On a second BLE-capable device, open nRF Connect (or similar BLE central tool) and scan for BLE devices.

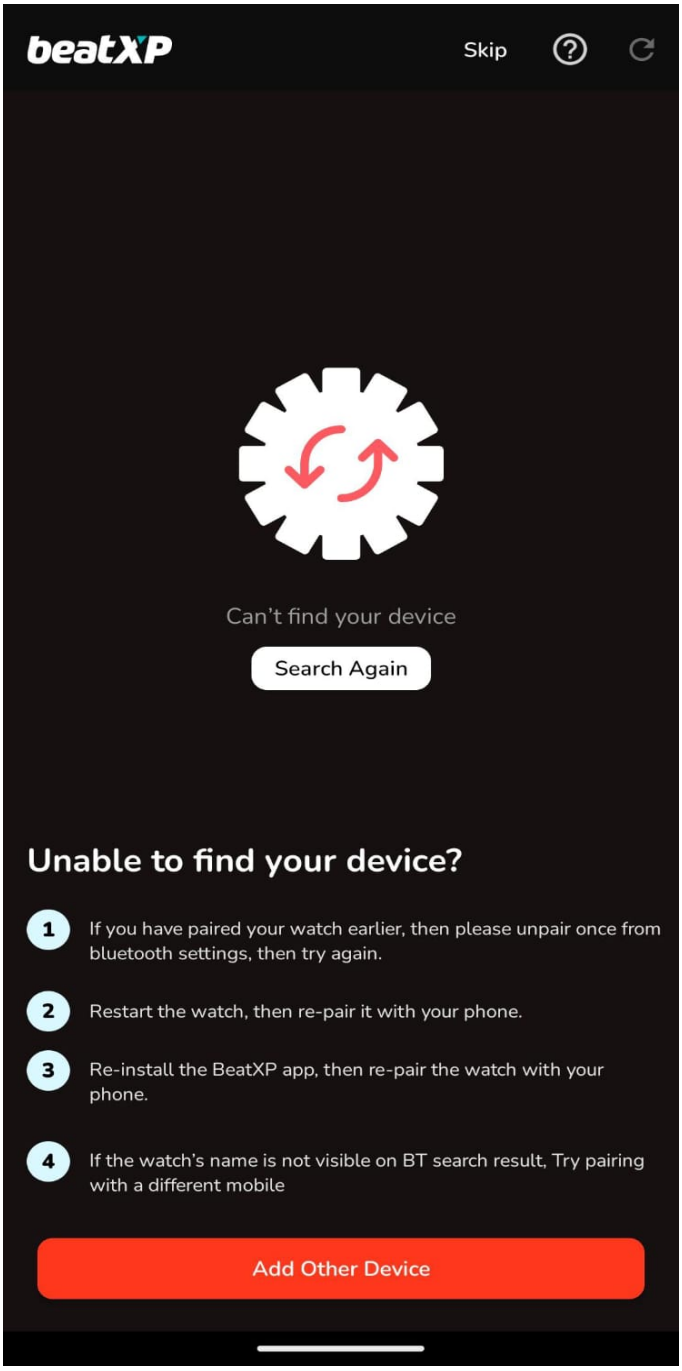


4. Identify the target Beat XP device in the scan results and establish a connection from nRF Connect.



5. Return to the companion app and attempt to connect to the Beat XP watch.

6. Observe that the companion app cannot discover or connect to the watch (the BLE interface is effectively locked by the unauthorized session).



7. While the unauthorized session remains active, the watch will not accept new BLE connections; device management and sync operations are blocked until the unauthorized central disconnects.

Notes

This proof-of-concept demonstrates availability impact only; no confidential data extraction or escalation was required to reproduce the condition. Reproduction requires physical proximity (BLE range) to the target device.

3 Remediation and Recommendations

Prioritized remediation steps:

1. **Enforce Pairing & Bonding:** Do not expose management/configuration GATT services until a secure pairing (with bonding) has been completed. Reject unauthenticated centrals for sensitive services.

2. **Implement Whitelisting:** Maintain a list of authorized centrals (by bonded keys or device identifiers). Refuse connection attempts for unrecognized centrals when connecting to sensitive services.

3. **Session Management Controls:** Allow multiple logical sessions or implement preemption: authorized companion apps should be able to request disconnection of stale or untrusted sessions. Add inactivity timeouts that automatically disconnect centrals that do not perform valid operations within a short interval.

4. **Operation-Based Validation:** Require a minimal authenticated action (e.g., signed/validated GATT handshake) within N seconds of connection; if not performed, disconnect.

4 Appendix — Contact and Disclosure

Reporter:	Nikhil Yalgar
Contact:	nik.sec127001@proton.me
Vendor Contact:	support@beatxp.com

Disclosure Note: This report is intended for responsible disclosure to Beat XP. The information contained herein is to be treated as confidential until a coordinated disclosure and remediation have been completed.