Security Advisory: BES2300 SBC Decoder Vulnerabilities

CVE ID: CVE-2026-79379
Vendor: Bestechnic Co., Ltd.
Product: BES2300 Bluetooth Audio SoC Firmware
Affected Versions: v3.x and earlier (2018–2019 releases, End-of-Life)
Fixed Versions: v5.0 / RC06 and later (released 2023-05-15)
Discoverer: Denis Goryushev, Positive Technologies
Vendor Acknowledgment: Confirmed

Overview

Two independent security vulnerabilities have been identified in the SBC audio codec decoder function `SBC_DecodeFrames()` of the Bestechnic BES2300 Bluetooth Audio SoC firmware (v3.x and earlier). Both vulnerabilities reside in the same function but are triggered through distinct code paths with different root causes and exploitation conditions.

The vulnerabilities are addressed in v5.0 / RC06 (released 15 May 2023) through a **complete architectural redesign** of the SBC decoder. No standalone patches are available for legacy branches; the supported remediation is upgrade to v5.0 / RC06 or later. Legacy versions (v3.x and earlier) have entered End-of-Life and will not receive backported fixes.

Vulnerability 1: TOCTOU Buffer Overflow

- **CWE**: CWE-367 (Time-of-check Time-of-use Race Condition), CWE-120 (Buffer Copy without Checking Size of Input)
- **CVSS v3.1**: `CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H` — **5.9 (Medium)**

Description

In the BES2300 Bluetooth audio SoC firmware (v3.x and earlier), the SBC audio codec decoder function `SBC_DecodeFrames()` processes multiple concatenated SBC frames from an A2DP audio stream in a single call. After decoding each frame, the synthesis filter writes PCM data into a global 0x2000-byte media buffer, with a logical boundary at 0xA00 (2560 bytes). A post-synthesis bounds check determines whether the next frame can be decoded by evaluating: if ((MaxPcmData - PcmData->dataLen) >= Decoder->maxPcmLen)

The flaw is a Time-of-Check to Time-of-Use (TOCTOU) vulnerability: the check uses the `maxPcmLen` value from the **previous frame (frame N)** to decide whether the **current frame (frame N+1)** will fit. However, each SBC frame carries its own header specifying channel mode, block count, and subband count, allowing `maxPcmLen` to vary from **32 bytes** (mono, 4 blocks, 4 subbands) to **512 bytes** (stereo, 16 blocks, 8 subbands) — a **16× range** fully controlled by the attacker via a single header byte.

By combining this with RTP `frame_num` spoofing (which forces multiple frames to be decoded within one invocation), an attacker can position a small frame (32 bytes) immediately before a large frame (512 bytes).

The bounds check passes using the small frame's size, but the subsequent write by `SbcSynthesisFilter4()` or `SbcSynthesisFilter8()` overflows past the 0xA00 boundary, corrupting adjacent global memory.

Technical Constraints

In the actual memory layout of the BES2300 firmware, the memory region affected by this overflow does not contain any function pointers, return addresses, or control-flow data. Consequently, while the overflow reliably causes a system crash (denial of service), **it cannot be leveraged for arbitrary code execution on this platform**.

Successful exploitation requires simultaneous satisfaction of multiple conditions:

- Spoof the RTP `frame_num` field
- Construct two SBC frames with differing parameters (small followed by large)
- Compute a valid CRC-8 checksum for each frame

These conditions significantly elevate the practical attack complexity.

Mitigation

The vulnerability is addressed in v5.0 / RC06 by a complete architectural redesign of the SBC decoder, which eliminates the TOCTOU flaw by performing bounds checking against the **current frame's** `maxPcmLen` before synthesis.

Vulnerability 2: Denial of Service via Reachable Assertion

- **CWE**: CWE-617 (Reachable Assertion), CWE-248 (Uncaught Exception)
- **CVSS v3.1**: `CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H` — **6.5 (Medium)**

Description

In the BES2300 Bluetooth audio SoC firmware (v3.x and earlier), the `SBC_DecodeFrames()` function contains multiple assertion checks that, when triggered, call `assertion_failed()` and enter an unrecoverable infinite loop, ultimately causing a system crash and triggering an automatic device reboot via the hardware watchdog. Audio service is interrupted; the device recovers automatically after reboot, and the Bluetooth connection must be re-established.

The vulnerability can be triggered in **two independent ways**:

1. Rapid configuration switching mid-stream

An attacker sends an A2DP stream that rapidly alternates SBC configuration parameters (e.g., joint stereo 8 subbands to mono 4 subbands). During synchronization scanning, the parser misidentifies a `0x9C` byte present in the audio data of the previous frame as a valid syncword (SBC frame header). This causes the parser to interpret garbage data as a frame header and compute an oversized `stageLen` value, exceeding the 512-byte staging buffer limit, which triggers the assertion.

2. High bitpool in dual-channel mode

When `numChannels=2`, `numBlocks=16`, and `bitPool >= 129`, the computation: frameBits = 16 × 2 × bitPool stageLen = frameBits / 8

For `bitPool = 129`, `stageLen = 516` bytes, which exceeds the fixed 512-byte staging buffer. This directly triggers the assertion without requiring configuration switching.

Impact Scope

This vulnerability is **limited to denial of service** and does **not** allow data exfiltration, privilege escalation, or code execution. The device recovers automatically via watchdog reboot, and the issue does not cause permanent damage to the device firmware.

Mitigation

The vulnerability is addressed in v5.0 / RC06 by a complete architectural redesign of the SBC decoder, which replaces the problematic assertions with proper error handling and removes the infinite loop, ensuring that malformed frames are discarded without system disruption.

Summary

Feature	Vulnerability 1	Vulnerability 2
CVE	CVE-2026-79379	CVE-2026-79379 (merged)
Root Cause	TOCTOU bounds check	Reachable assertion
Trigger	frame_num spoofing + frame size variation	Config switching OR bitPool >= 129
CRC Required	Yes	No
Impact	System crash (DoS)	Watchdog reboot (DoS)
RCE Possible	No (memory layout constraint)	No
CVSS	5.9 (Medium)	6.5 (Medium)

Recommended Actions

1. **Upgrade to v5.0 / RC06 or later** — This is the only supported remediation. The SBC decoder has been completely redesigned to eliminate both vulnerabilities.
2. **For legacy users unable to upgrade immediately**:
    - Limit SBC decoding to trusted audio sources
    - Consider disabling A2DP Sink functionality if not business-critical
3. **Note**: Legacy versions (v3.x and earlier) have entered End-of-Life and will not receive backported fixes.

Credit

These vulnerabilities were discovered by **Denis Goryushev** of **Positive Technologies**.

References

- Vendor Product Page: http://bestechnic.com
- CVE Entry: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2026-79379

This advisory was prepared by Bestechnic Co., Ltd. in coordination with the discoverer.