CVE-2026–31280: Insecure Bluetooth "RFCOMM" Leading to Device Crash in Parani M10 Intercom

Device: Parani M10 Intercom Firmware Version:V2.1.3 Company Name: Parani India (Backed by Sena technologies Inc.)

1 Security Assessment Details

1.1 Executive Summary

This vulnerability impacts device availability, integrity and confidentiality due to the
exposure of an unauthenticated Bluetooth Classic RFCOMM service combined with improper input validation. The device allows un-authenticated connection by bypassing
of enabling pairing mode within Bluetooth range to establish a session and send unauthorized commands. A threat actor can disrupt normal operation by injecting arbitrary
audio or sending malicious input that triggers Man-In-Middle(MITM), buffer overflow
which are leads to device crash, disrupt authorized Bluetooth connection.

1.2 Scope and Objectives

The scope of this assessment was limited to Bluetooth Classic Communication of Parani
M10 Intercom(Firmware Version 2.1.3).

1.3 Technology Impact Summary

The security assessment of the Bluetooth Classic communication interface has been performed. These assessments aimed to identify security weaknesses in the evaluated intercom device, explain the impact and associated risks, and provide guidance for prioritization and remediation.

Following are the technical impacts:

An attacker within Bluetooth range can connect to an exposed RFCOMM service without
authentication and perform unauthorized actions, including sending of arbitrary payloads
leads to device crash until next manual intervention. Also attacker do MITM causes to
play arbitrary audio discontinue authorized connection between user mobile Intercom
device.

1.4 Business Impact Summary

1.4.1 Overall Business Impact

The identified wireless-layer vulnerability represents a significant high business risk,
as successful exploitation could disrupt normal device operation, allow unauthorized malicious data injection, negatively impact customer trust and user experience, damage
brand reputation and market credibility, introduce safety concerns in sensitive deployment environments, and potentially expose the organization to regulatory scrutiny, legal
liability, and financial costs associated with remediation and customer support.

1.5 Testing Environment and Tools

Bluetooth security testing was conducted using standard Bluetooth enumeration and
interaction tools:

• The intercom device equipped with Bluetooth Classic functionality
• A Linux-based security testing workstation (Kali Linux) with TP -Link Bluetooth
adapter for Bluetooth connectivity testing.
• “bluetoothctl” CLI tool for pairing analysis and service enumeration.
• “RFCOMM” utilities used for establish direct channel communication and transmit
crafted test payloads.
• “btmon” utility used to capture logs for analysis and service enumeration.
• A python Script for payloads flooding.

1.6 Table of Findings

Finding ID	Scope	Finding	CVSS Score	CVSS Vector	Severity	Status
PM10-IBT-01	Bluetooth Classic	Insecure Bluetooth Communia-tion	8.6	CVSS:4.0 / AV:A / AC:L / AT:N / PR:N / UI:P / VC:H / VI:H / VA:H / SC:N / SI:N / SA:N	High	Not Fixed

1.7 Device Strengths

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

1.8 Device Weaknesses

• The intercom device exposes an unauthenticated Bluetooth Classic RFCOMM service, allowing unauthorized nearby attackers to establish a connection bypassing of
enabling pairing mode on the device. This leads to create buffer overflow conditions
further that can result in device crash or reboot until manual intervention.

• The exposure of RFCOMM channels (CH10, CH12) in the device makes attacker
to create a MITM environment. It discontinue authorized user establishment which
disrupt Bluetooth communications by playing arbitrary noise or crash the device.

2 Technical Findings

2.1 PM10-IBT-01: Insecure Bluetooth Communiation

Potential Impact: High

Description

The intercom device relies on Bluetooth Classic communication to provide local wireless functionality. During the assessment, it was observed that the device exposes an
RFCOMM service without requiring pairing or authentication. A threat actor within
Bluetooth range can establish a direct connection to the device and transmit unauthorized commands. It was further identified that the RFCOMM service does not properly
validate input length. By sending malicious data, the attacker can trigger a buffer overflow condition, causing the device to crash or reboot. Additionally, unauthorized audio
playback can be performed, disrupting normal device behavior

Affected Components

• The device’s Bluetooth Classic communication module.
• The exposed RFCOMM service interface.
• The command-processing and input-handling mechanism within the firmware.

Technical Risk

An attacker can establish an unauthenticated connection and inject arbitrary commands,
impacting device integrity. Additionally, exploitation of the buffer overflow condition can
cause the device to become unavailable resulting in Denial-of-Service state until physical
intervention to restore normal functionality.

Business Risk

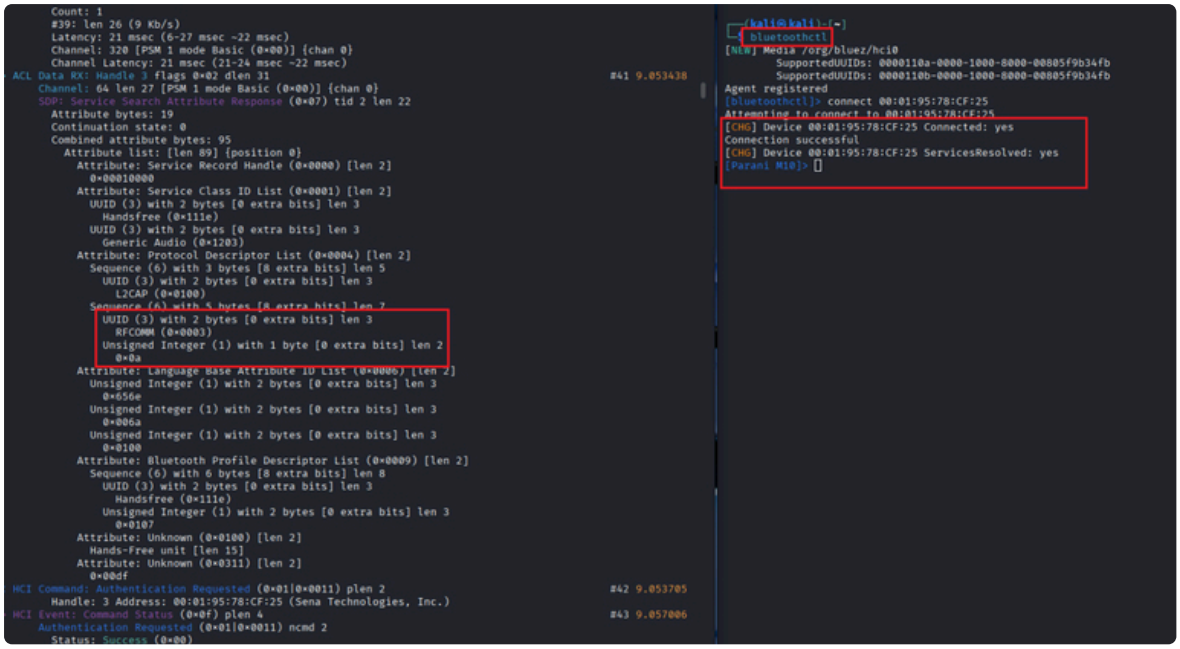
Exploitation of this vulnerability could:

- Lead to operational downtime or instability of the device
- Increase customer dissatisfaction and operational support costs
- Negatively affect brand reputation and long-term consumer trust

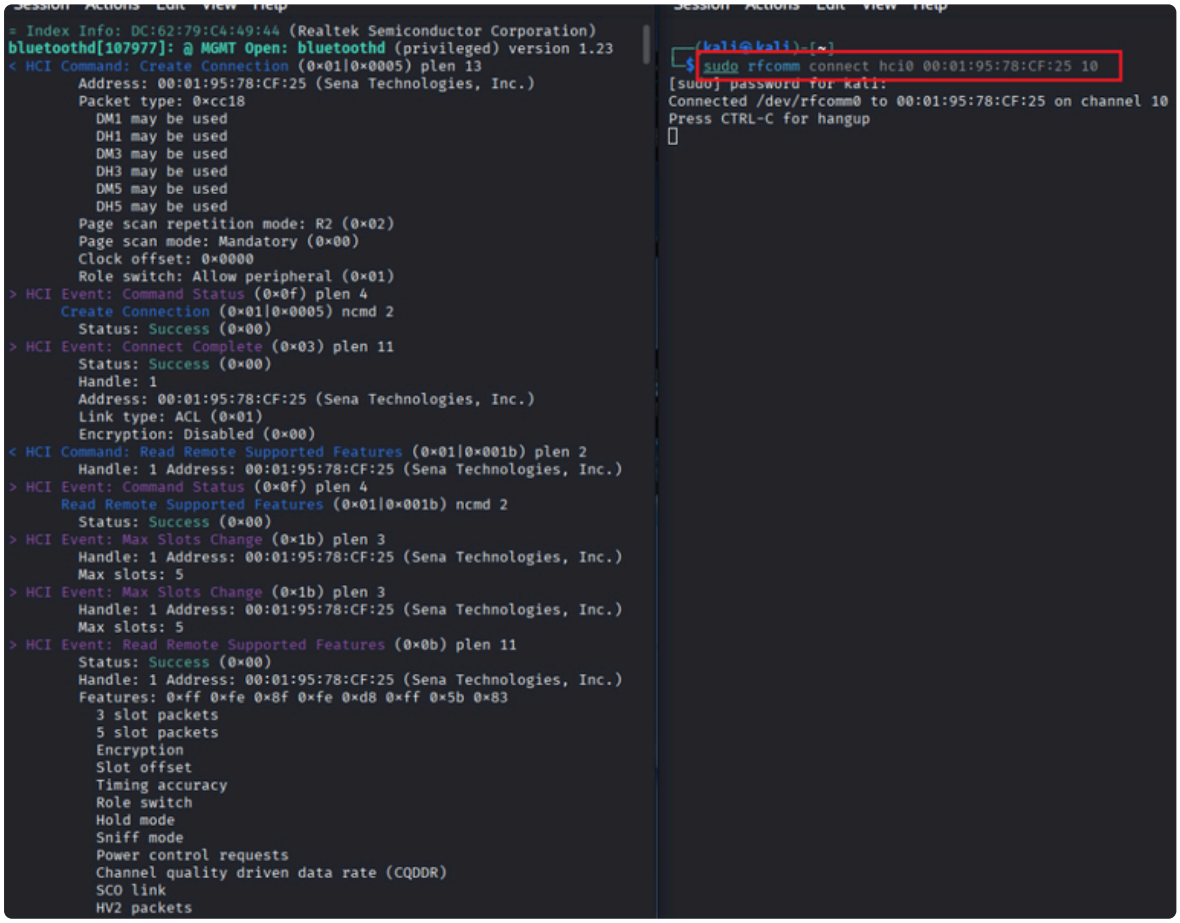
Steps to Reproduce (High-Level) Case 1 - Buffer Overflow Attack

1. Perform OSINT on Target Device: Conduct open-source intelligence (OSINT) to gather publicly available information related to the intercom device, including identification of its Bluetooth MAC address.
2. Validate Device MAC Address: Physically inspect the intercom device and confirm that the Bluetooth MAC address identified during OSINT matches the MAC address printed on the back label of the device.

3. Assess Pairing Configuration: Attempt to pair with the device and observe that it allows pairing without requiring authentication or user verification.
4. Enumerate Available Services Post-Pairing: After establishing the unauthenticated pairing, review the list of exposed Bluetooth services and identify that an RFCOMM service is active on channel 10 and 12.



5. Establish RFCOMM Connection: Initiate a direct RFCOMM connection to channel 10 using appropriate Bluetooth utilities.

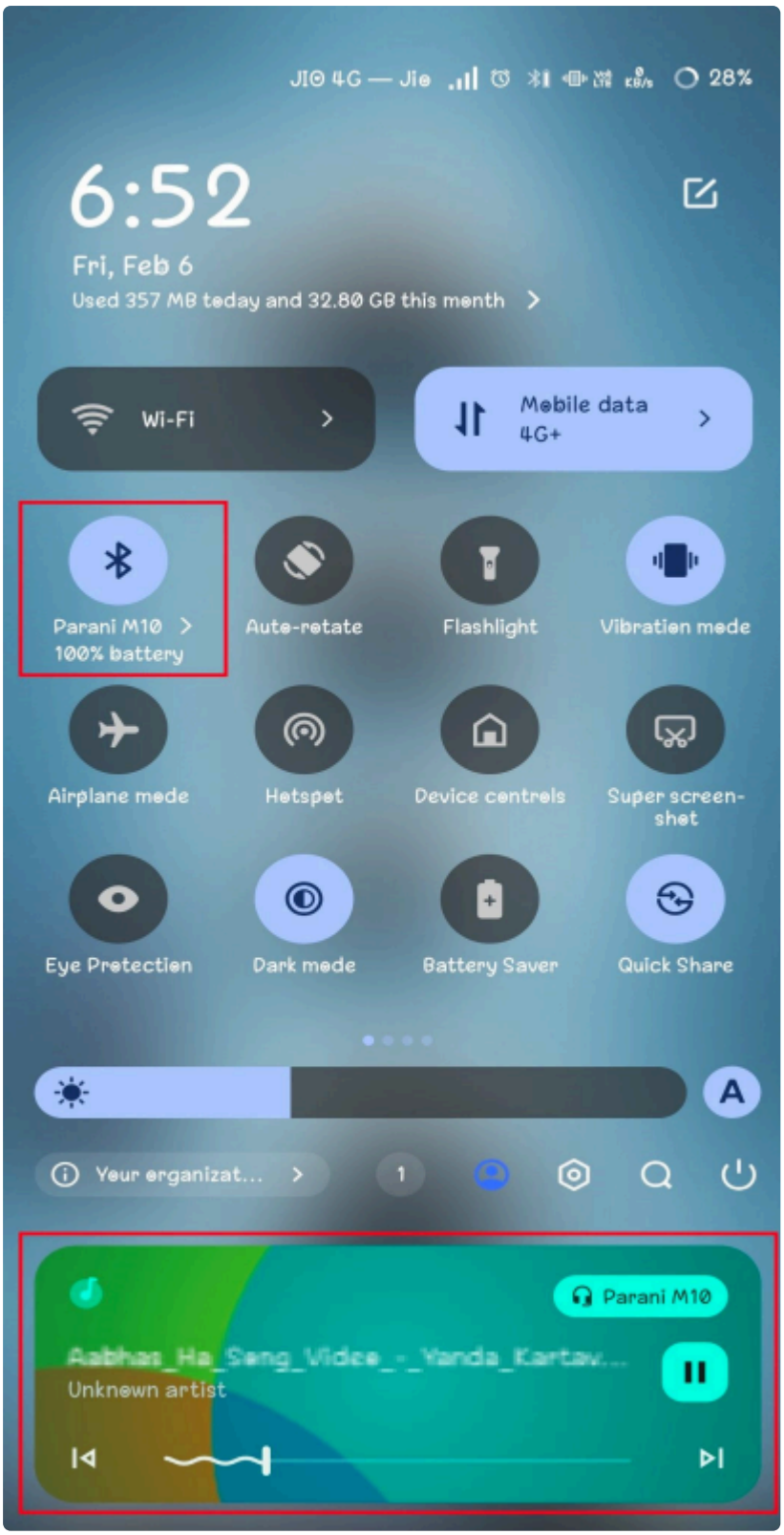


6. Execute Crafted Script: Run a specially crafted script to transmit unauthorized and oversized input data through the established RFCOMM session.

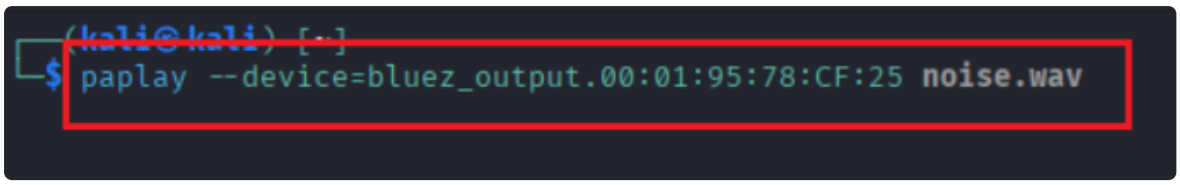
7. Observe that the device accepts the injected input and subsequently crashes or powered off, confirming the presence of an unauthenticated command injection vulnerability combined with a buffer overflow condition.

Case 2- Man In the Middle Attack

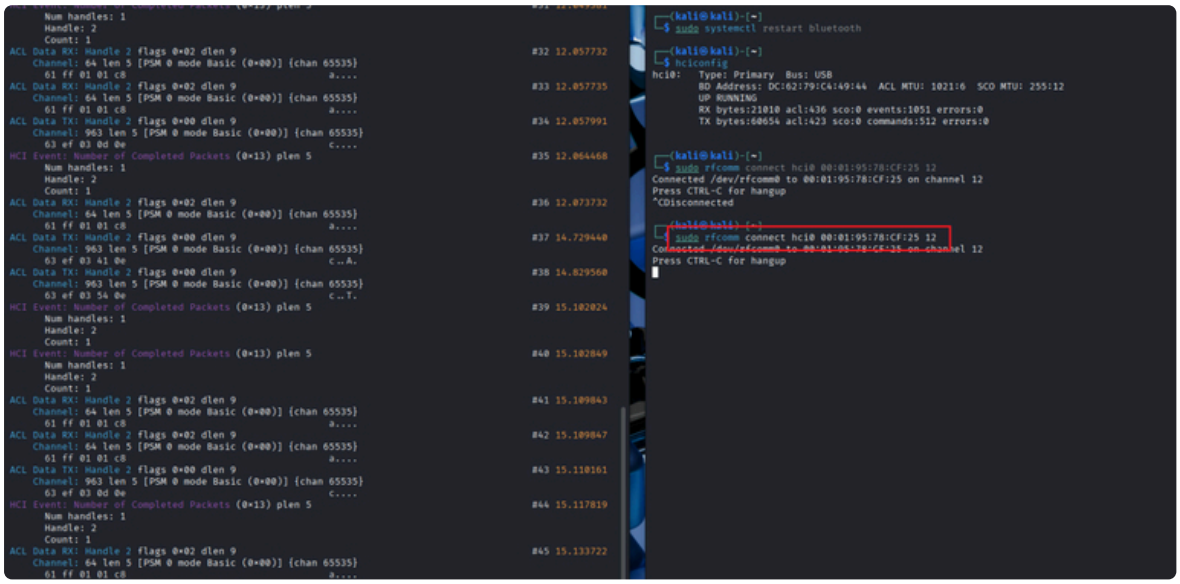
1. Connect the mobile phone to the intercom via Bluetooth and begin playing an audio track to confirm a stable connection.



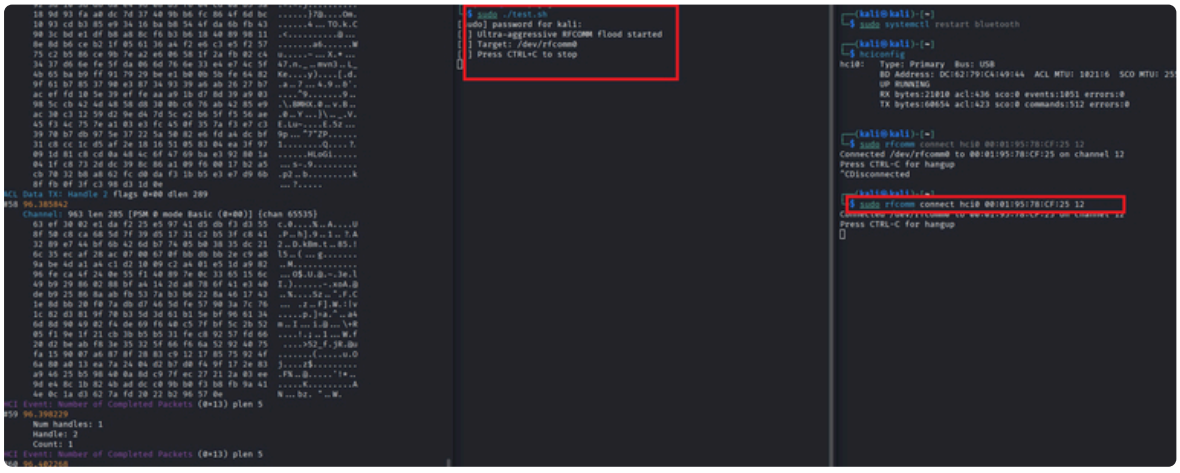
2. Audio data was injected into the intercom stream through the Paplay utility.The attack succeeded, resulting in arbitrary audio being played over the intercom through an unauthorized method.



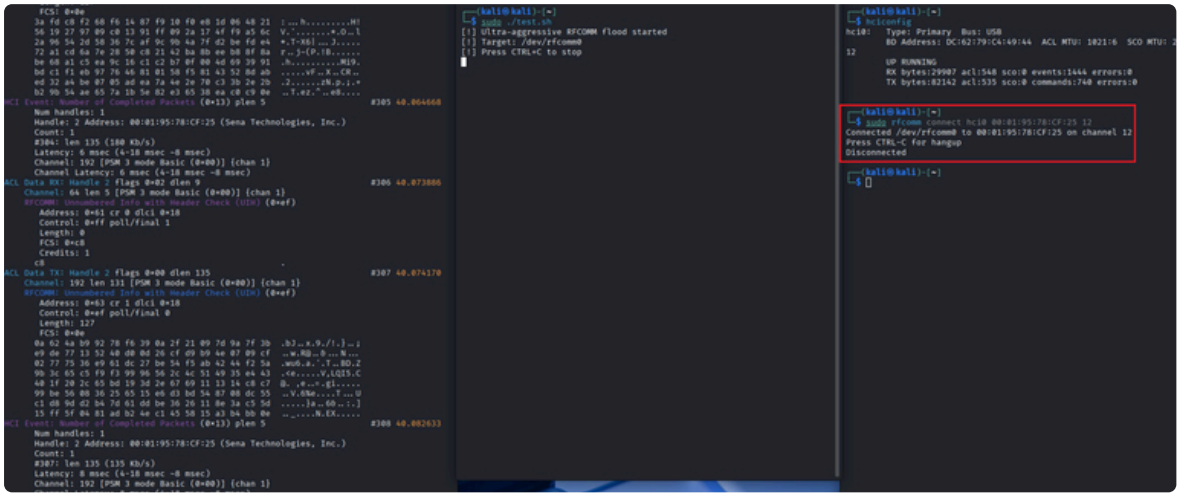
3. Establish an RFCOMM connection to the intercom using an available channel 12.

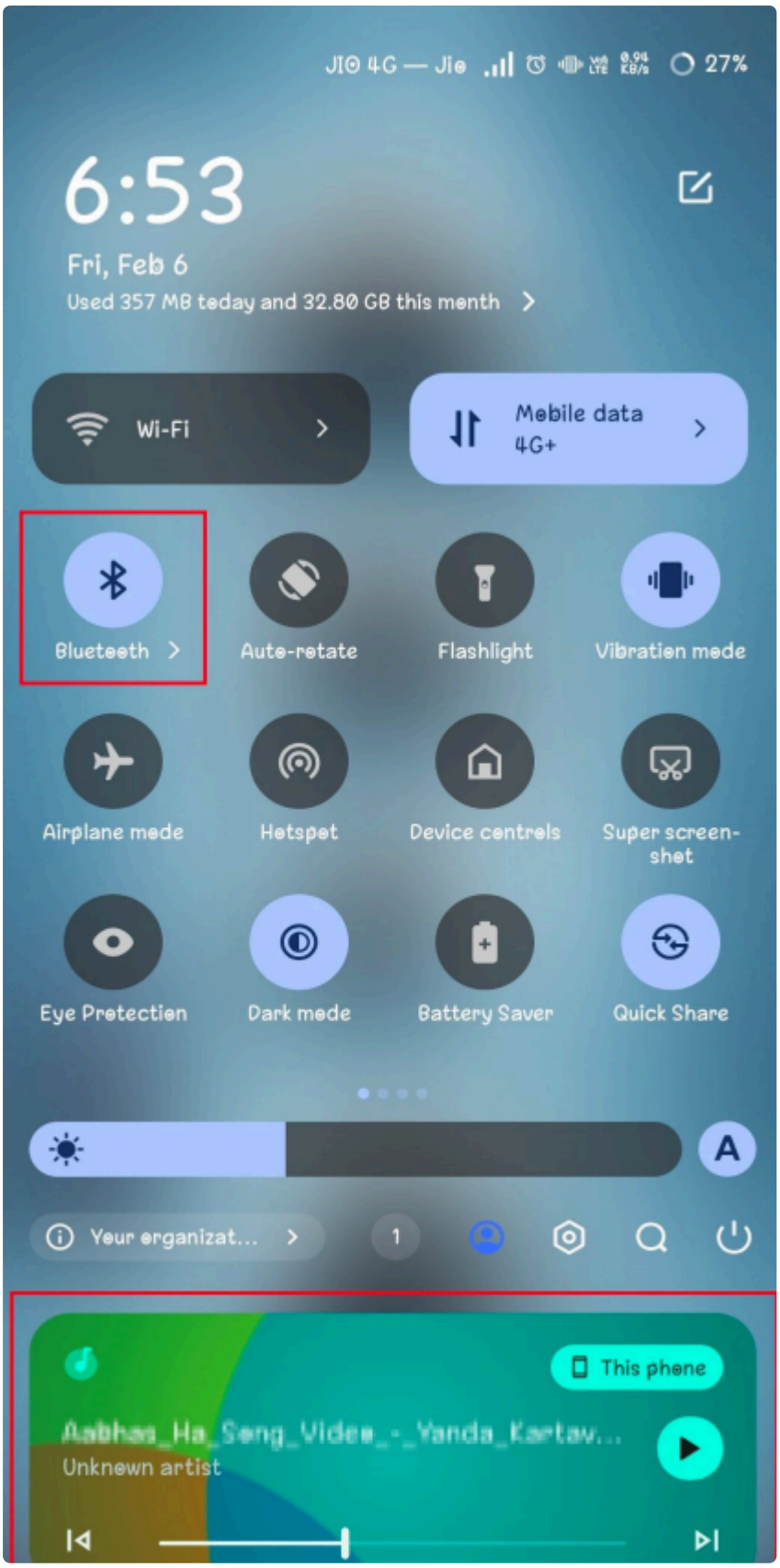


4. Conduct a Denial-of-Service (DoS) attack over RFCOMM. Upon successfull execution of attack, the connected mobile device was forcibly disconnected. Additionally,
other intercom devices connected to the same unit were also disconnected. The target intercom crashes, and remaining non-functional until manual intervention is
performed.



5. It was observed that the mobile device was successfully disconnected from the intercom, and the intercom became unavailable for further connections until manual
intervention is performed.




JIO 4G — Jio
27%
6:53
Fri, Feb 6
Used 357 MB today and 32.80 GB this month
Wi-Fi
Mobile data
4G+
Bluetooth
Auto-rotate
Flashlight
Vibration mode
Airplane mode
Hotspot
Device controls
Super screen-shot
Eye Protection
Dark mode
Battery Saver
Quick Share
A
Your organizat...
1
This phone
Unknown artist

Notes

This proof-of-concept was conducted in a controlled and authorized testing environment.
The assessment was limited to demonstrating unauthenticated command injection and
service disruption through a buffer overflow condition over Bluetooth Classic communication. No attempts were made to perform advanced exploitation beyond validating the
identified vulnerability.

3 Remediation and Recommendations

• Enforce Secure Authentication and Pairing Controls: Configure the Bluetooth interface to require authenticated pairing (e.g., Secure Simple Pairing with user confirmation) before granting access to any services.
• Implement Service-Level Authorization: Restrict access to the RFCOMM service
by validating authenticated link keys and enforcing authorization checks prior to
processing commands.
• Strengthen Input Validation Mechanisms: Implement strict bounds checking and
proper input length validation within the RFCOMM service handler to prevent buffer overflow conditions.

4 Appendix — Contact and Disclosure

Researcher(s): Tapadyuti Baral, Nikhil Yalgar
Contact: arghyabaral@gmail.com, nik.sec127001@proton.me

Previous
Finding Hardcoded Telnet Credentials

Last updated 29 days ago