Bluetooth Channel Penetration Test Report

ALHAMRANI UNIVERSAL

SISA Information Security

Global Service Centre

SISA House, 3029,

Sri Sai Darshan Marg,

13th Main, HAL II Stage,

Indiranagar, Bangalore, India.

We are pleased to announce that we have completed the **Bluetooth Channel Penetration Test** for **ALHAMRANI UNIVERSAL**. We have enclosed the detailed findings and recommendations.

We value the opportunity to work with you and appreciate the cooperation provided to us during the penetration testing activity. We would be pleased to discuss any further clarifications with respect to the report and please feel free to revert to us.

Yours sincerely,

Technical Security Services

SISA Information Security

Table of Contents

1. Report Summary

Title	Bluetooth Channel Penetration Test Report
Date	June 2018
Version History	Application Penetration Test Report v1.1
Author	SISA Information Security

1.1 Scope of the Penetration Test

Organization	ALHAMRANI UNIVERSAL
Time Frame	6th April 2018 – 29th June 2018
Application/IP Tested	Bluetooth Channel
Device	MPOS – Ingenico Link/2500

2. Executive Summary

2.1 Introduction

SISA Information Security, an Information security specialist firm conducted the **Bluetooth Channel Penetration Test** for **ALHAMRANI UNIVERSAL**. The penetration test was conducted with the tools and techniques that the malicious hacker uses to compromise the information with respect to Confidentiality, Integrity and Availability of the application.

The aim of the penetration test (pen test), also called ethical hacking, is to simulate an attack on the Mobile application to uncover all security issues of the application and of the data stored by it. By doing a controlled simulation of an attack, a penetration test uncovers security flaws in a realistic way. The attacking methods are also varied and range from passive scanning to targeted automated and manual attacks to exploit a specific vulnerability.

The penetration test was conducted by SISA consultants from **6th April 2018 – 20th April 2018**. The revalidation to confirm the closure of reported issues was conducted on **29th June 2018**.

2.2 Vulnerability Level Classification

Individual Vulnerability Rating – It should be noted that the overall business risk caused by any of the issues found is outside our scope. This means that some risk reported as high from a technical perspective may be considered as medium, low or acceptable, as a result of other compensating controls unknown to us. Individual vulnerability should calculate on the basis of three properties.

Impact on the business	How the business will be affected if that particular vulnerability is exploited.
Ease of exploitation	Skill level required to exploit the vulnerability like skilled, moderate or script kiddies.
Exposure	What is the exposure of application for example it is available for public user, registered user or only internal users.

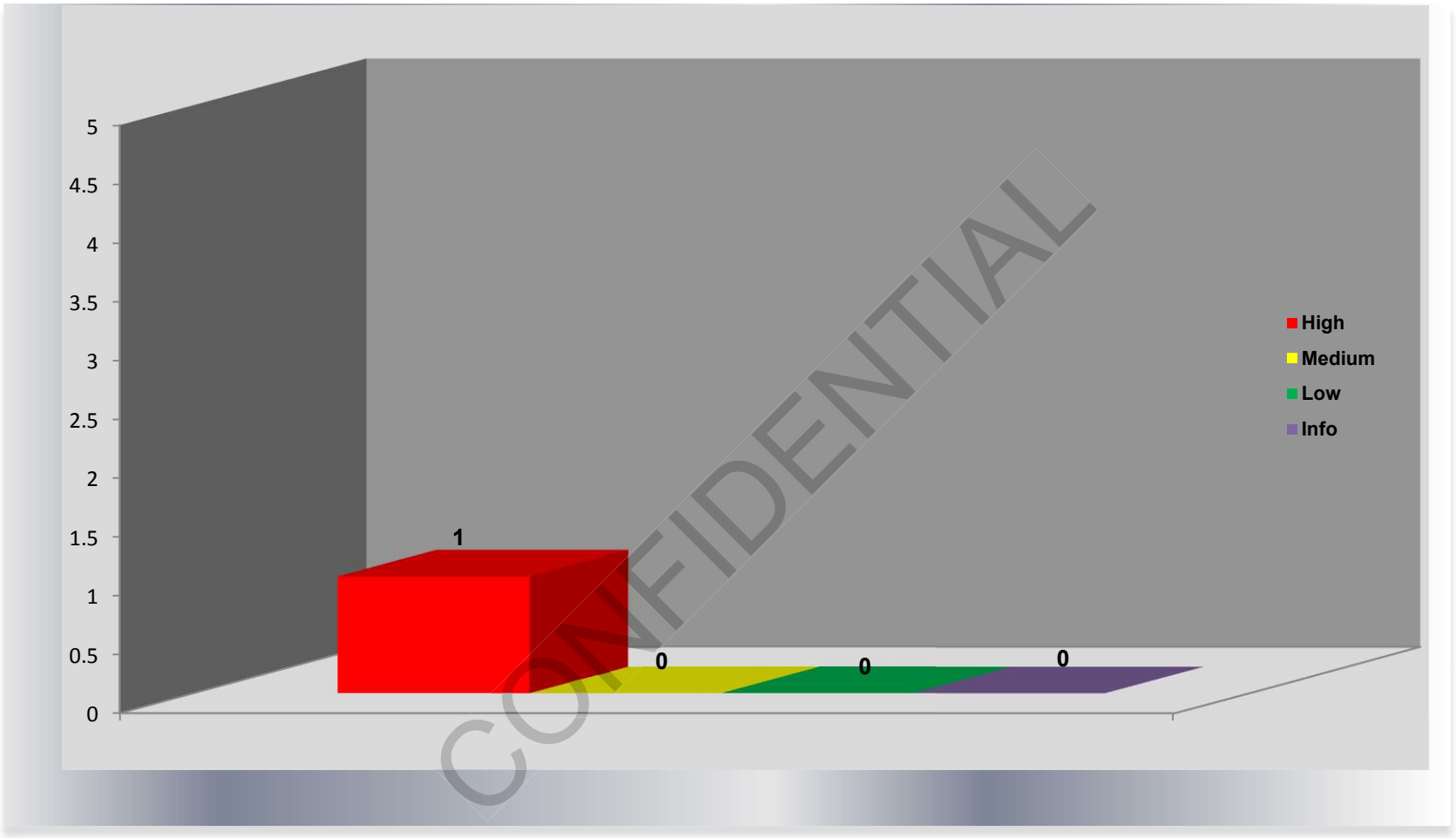
Risk Level	Description
High	**High Risk** vulnerability can be exploited by an intruder to get full administrative access to the application or its primary operating system.
Medium	**Medium Risk** vulnerability discloses information about the application and its underlying communications that can be used by an attacker in conjunction with another vulnerability to gain administrative power on the application or its primary operating system.
Low	**Low Risk** vulnerability can result in inventory of vital information held by or about the application or its primary operating system.

2.3 Overall Findings

SISA has covered all possible tests, initiated from the automated tools, and finished with manual testing and exploitation attempts. The overall assessment summary is as below:

Number of Applications/URLs Tested	**1**
Total Number of Vulnerabilities Discovered	**1**
High Severity	**1**
Medium Severity	**0**
Low Severity	**0**
Informational	**0**

2.4 Graphical Summary of Findings



3. Findings Summary

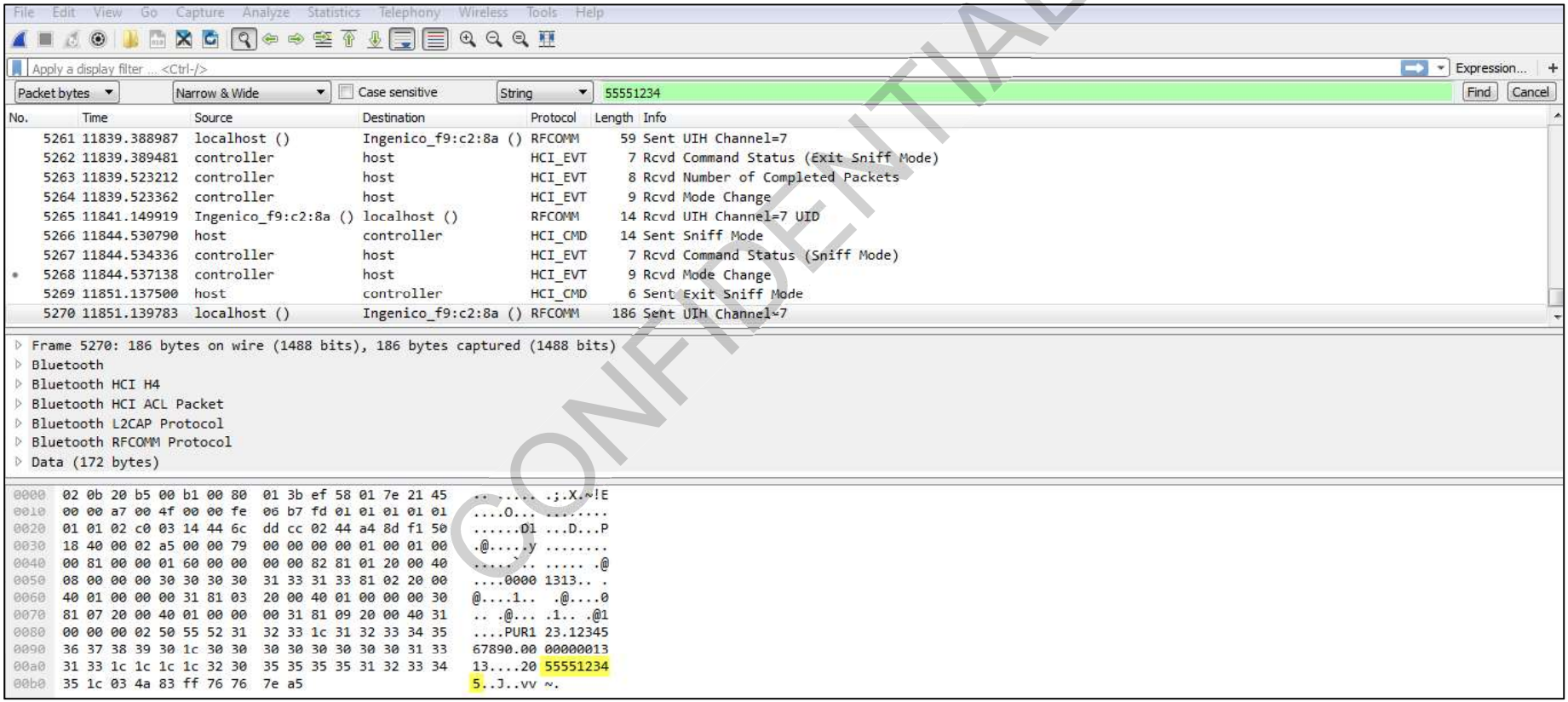
Sr. No.	Vulnerability Name	Affected Platform	Severity Level	Result
1.	Unencrypted Data Transmission	Blutooth Channel	High	CLOSED

4. Test Details

4.1 Unencrypted Data Transmission

In order to secure data that is being transferred, TLS/SSL makes use of one or more cipher suites. Transmission of data in plain text is vulnerable to eavesdropping and Man In the Middle attack, resulting in the sniffing of sensitive data.

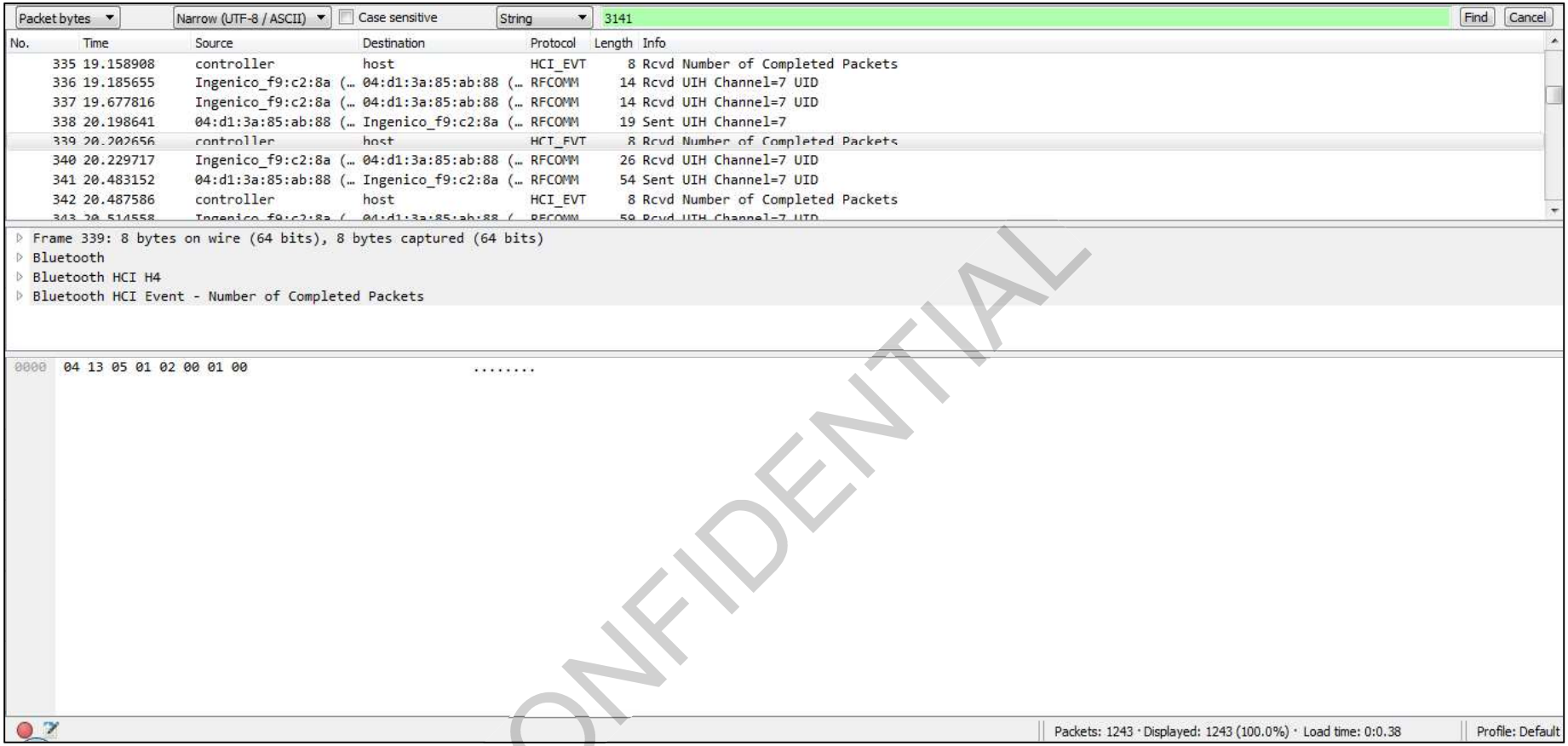
Proof of Concept:



Recommendation:

Encryption must be enabled for the Bluetooth data communication.

Proof of Concept after Fix:



Conclusion:

After fix, user data is transmitted using secure encrypted channel to avoid sniffing of the data.

5. Risk Rating

The Technical Security Services team at SISA Information Security has performed the **Bluetooth Channel Penetration Test** for **ALHAMRANI UNIVERSAL**.

The overall current security posture of the application is **GOOD**.

Yours truly,

Technical Security Services

SISA Information Security

Date: 29th June 2018

6. Appendix

6.1 Test Approach

Bluetooth Penetration Test is an attack simulation that is intended to expose the effectiveness of an application's security controls by highlighting risks posed by actual exploitable vulnerabilities. The testing model is built around a manual testing process. This process is intended to go much further than the generic responses, false positive findings, and lack of depth provided by automated application assessment tools.