Le BonBon Croissant
Penetration Test Briefing

FINALS-XX

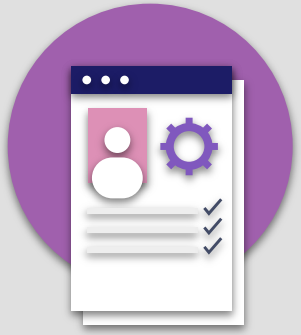
// Confidential - For LBC$_{LLC}$ Authorized Personnel Only //

Team Introduction

- XXXX XXXXX
- XXXX XXXXX
- XXXX XXXXX
- XXXX XXXXX
- XXXX XXXXX
- XXXX XXXXX

AGENDA

Risk Assessment

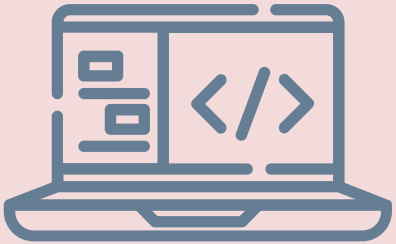


Regulatory Compliance Standards & Guidelines

Mitigation and Response

RISK ASSESSMENT

Scoring Methodology

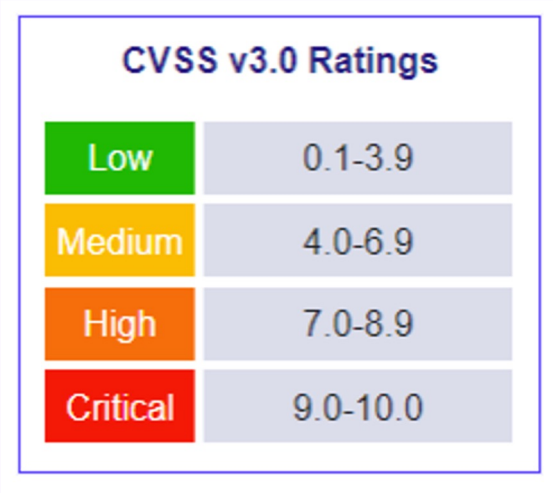


Hands-On Engagement

Findings

OUR SCORING METHODOLOGY

- 0.0 - 10.0 Scale
- Scoring Severity
- Overall, Impact, Exploitability



SUMMARY OF VULNERABILITIES

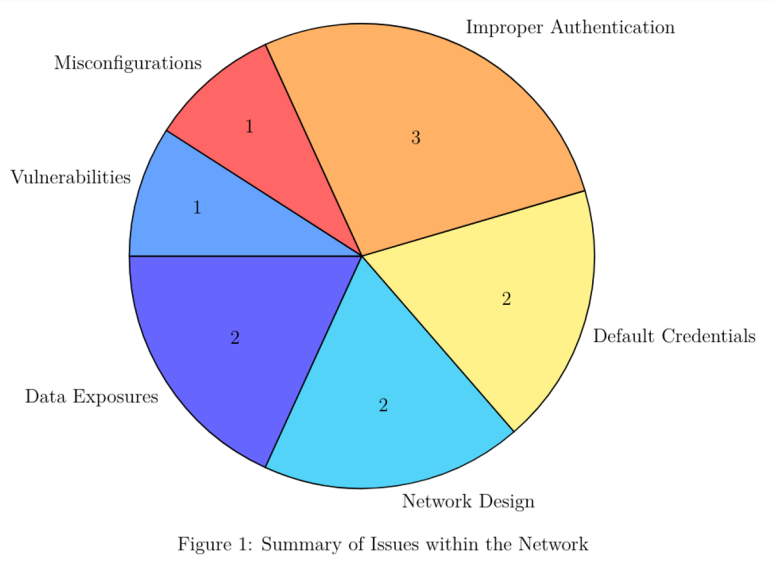


Figure 1: Summary of Issues within the Network

- 3 Improper Authentication
- 2 Default Credentials
- 2 Network Design
- 2 Data Exposures
- 1 Vulnerability
- 1 Misconfiguration

KEY FINDINGS

Default Credentials (SCADA)

- Allow access to critical ICS infrastructure

Lack of Authentication

- Access to sensitive information including credit card data and passwords
- Enables remote code execution

Lack of Network Segmentation

- Industrial systems can be tampered with
- Potential loss of life or revenue

HIGH FINDINGS

Lack of PLC Authentication

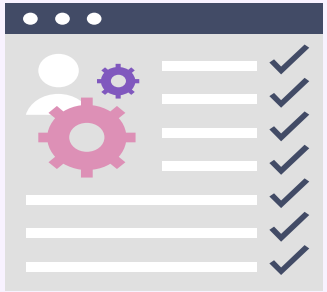
- Set ICS values to dangerous levels or deny service

Lack of MariaDB Authentication

- Access to Marketplace user passwords

PostgreSQL Database Remote Code Execution

- Full access of all databases on machine
- Full control (modification, deletion, etc.) of data stored within the host



MEDIUM FINDINGS

Payment Transaction Enumeration

- Extract user transactions
- View revenue

COMPLIANCE

REGULATORY COMPLIANCE & PENALTIES

PCI DSS

Review

Analyze

Report

REGULATORY COMPLIANCE & PENALTIES

Data Protection and Privacy Act (DPA)

Law No. 2016/1321

Application Decree 2005-1309

Privacy and Electronics Communications Regulations (PECR)

Application Decree 2019-341

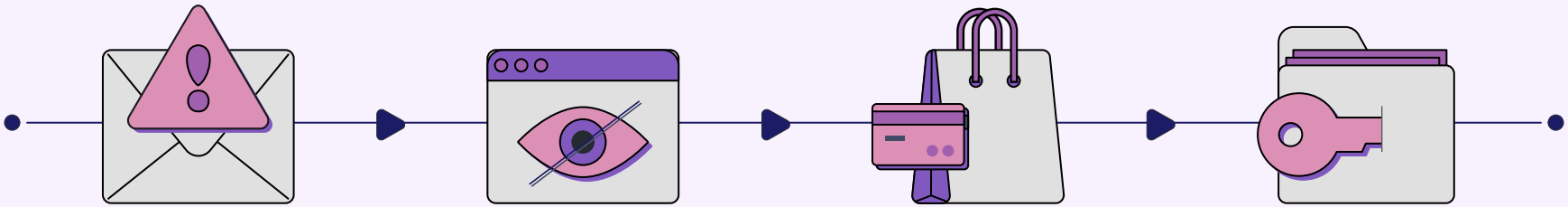
PCI-DSS v3

PCI-DSS COMPLIANCE

LBC was found to have over 40 PCI-DSS violations

MITIGATION AND RESPONSE

ORGANIZATIONAL IMPACT



Loss of Reputation

Reduced Revenue

Customer Data Breaches

Lawsuits or Bankruptcy

REMEDIATION

Suggestions

01

Least Privileges

Accounts should only access what they need

02

Implement Firewalls

To reduce potential vulnerabilities

03

SCADA Access Controls

To protect LBC's business operations

04

Password Policies

To improve protection of customer accounts

QUESTIONS?

Thank you for your time.