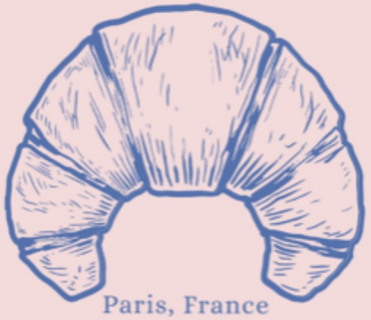
Le Bonbon Croissant

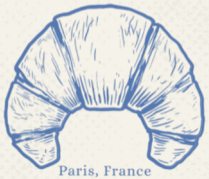
Penetration Test Executive Report



Team XX

Engagement Overview

- January 7th-8th, 2022
- Goals
  - Ensure security of industrial control systems and sensitive customer data
  - Evaluate e-commerce infrastructure and PCI DSS compliance
  - Investigate technical implementation of customer rewards program

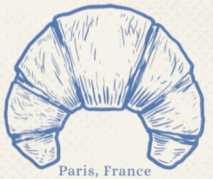


Methodology

CVSS

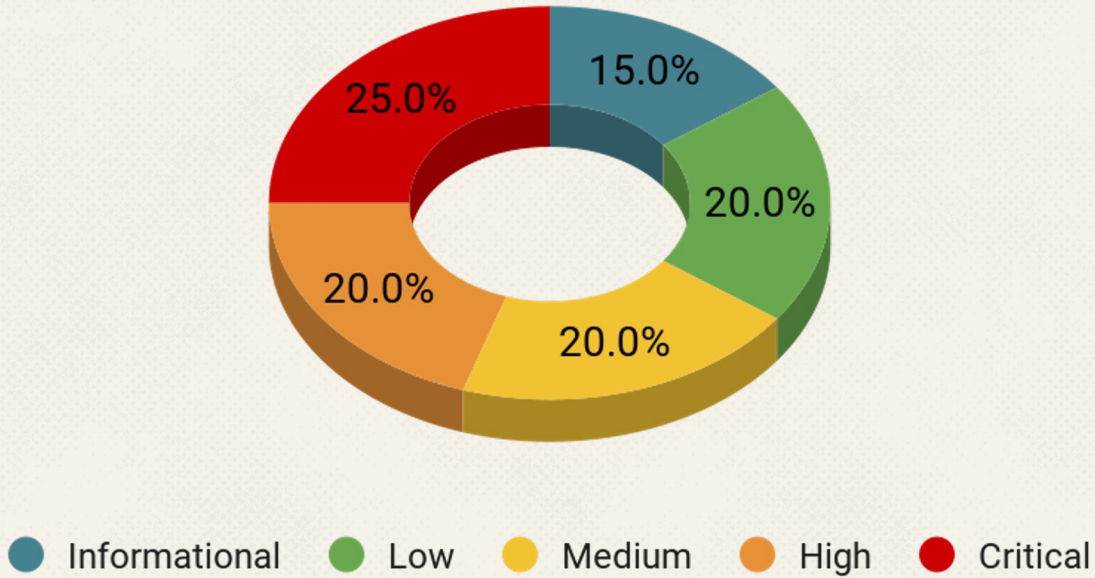
Eg. AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Severity	Base Score Range
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0



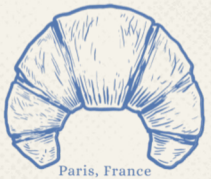
Risk Metrics

Findings by Severity



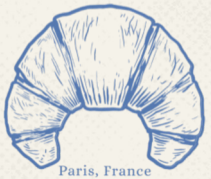
PCI DSS

Requirement Number	Requirement	Goal
6	Develop and maintain secure systems and applications	Maintain a Vulnerability Management Program
11	Regularly test security systems and processes	Regularly Monitor and Test Networks
12	Maintain a policy that addresses information security for all personnel	Maintain an Information Security Policy



PCI DSS

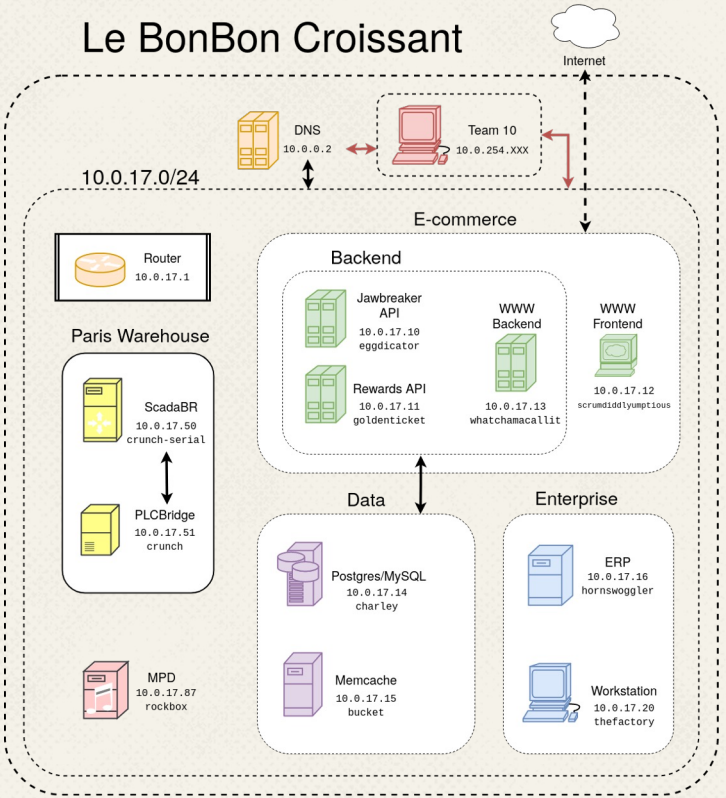
Requirement Number	Requirement	Goal
2	Do not use vendor-supplied defaults for system passwords and other security parameters	Build and maintain a secure network and systems
3	Protect stored cardholder data	Protect cardholder cata
5	Protect all systems against malware and regularly update antivirus software or programs	Maintain vulnerability management program
8	Identify and authenticate access to system components	Implement strong access control

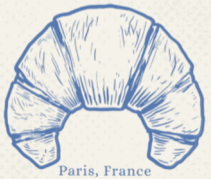


Findings

Key Strengths

- Encapsulation
  - Easy segmentation
- HTTPS remediation
- Reduced external services



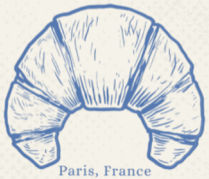


Key Findings

Default Credentials

ScadaBR Default Credentials
CVSS Rating 10.0
AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Database Default Credentials
CVSS Rating 8.1
AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

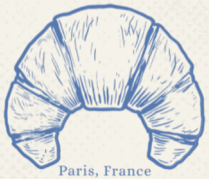


Key Findings

Remote Code Execution

ScadaBR Remote Code Execution
CVSS Rating 9.3
AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Postgres Remote Code Execution
CVSS Rating 7.9
AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:H



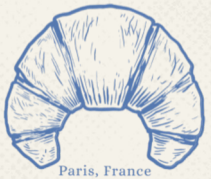
Key Findings

External Access

Unauthenticated PLC Communication
CVSS Rating 9.6
AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Arbitrary Rewards Account Creation
CVSS Rating 7.5
AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

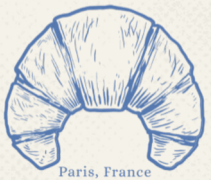
No PostgreSQL Access Filtering
CVSS Rating 6.5
AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N



Conclusions

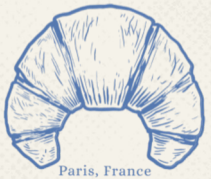
Impact

- Root access on automation controller
- Full access to user information database
  - Credit cards
  - User logins
- Exploitation of rewards program API



Recommendations

- ICS Security
  - No default passwords
  - Isolation and authorization
- Compliance
  - PCI DSS
- Rewards Program
  - Application-level authentication for web APIs



Questions?

The Team

XXXX XXXXX, Captain and Communications Manager

XXXX XXXXX, Compliance Specialist

XXXX XXXXX, Reverse Engineering Expert

XXXX XXXXX, Open Sourceror

XXXX XXXXX, Network Analyst

XXXX XXXXX, Cryptography and Credentials Specialist