The Cozy Croissant

Team Finals-XX

Penetration Test Executive Briefing

1 / 15 / 2023

Meet The Team

Agenda

1. Assessment Overview

2. Key strengths

3. Key Findings

4. Remediation Assessment

5. Compliance & Business Impact

6. Remediations and strategic recommendations

Assessment overview

Engagement objectives:

1 - Assessment of **applications** and **COTS software**

2 - Assessment of **active directory** environment and **access controls**

3 - Evaluation of **data storage, encryption,** and **private data** handling methodologies

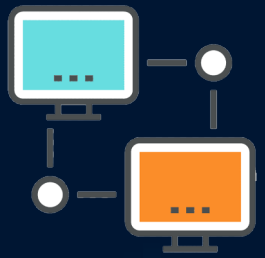
4 - Evaluating compliance with security **best practices and standards**

5 - Evaluation of **remediation effectiveness** based on previous findings

Scope and assessment methodology

Scope

Networks 10.0.0.0/24 and 10.0.200.0/24 consisting of 20 hosts.



Methodology

Adopted industry & American standard NIST-800-115

Scoring

Adopted F.I.R.S.T industry & American standard CVSS 3.1

Key strengths

Finals-5 identified several strong security controls within The Cozy Croissant.

Security Control	Description
Network Segmentation	Guest and corporate network are efficiently segmented and prevents internal pivoting
Firewall Security & ACL	Prior to expanded access granted, scanning probes could not bypass firewalls
Social Engineering Awareness	The frontdesk, if aware, did not provide requested information without proper clearance even considering the urgency, despite the information being there.

Key Findings

JellyFin media susceptible to DoS		CVSS SCORE	PRIORITIZATION
Risk	Critical	9.5 Critical	CAT-4
Impact	Very High		
Likelihood	High		

Description

The host 10.0.0.20 maintains the movie service for guests which is essential for the entertainment of the guests. This service contributes heavily to the rating of the establishment and thus, crucial for customer satisfaction and revenue generation. An exploit was discovered where specifying an enormous folder, such as the root of the entire system will overload the server and take it down. This will affect customers, TCC ratings, revenues and overall impact the reputation of TCC at maintaining customer satisfaction.

Key Findings

Exposed Payment API		CVSS SCORE	PRIORITIZATION
Risk	Critical	8.3 High	CAT-4
Impact	Very High		
Likelihood	Very High		

Description

The payment API defines the commands that are used to interact with payment data such as billing. For instance, it defines actions such as retrieving all bills, deleting a bill, adding a bill etc. Given this, adversary access to such an API essentially provides them with an instruction set on how to manipulate payment information. Various business impacts can be considered such as disruption of the financial department activities, loss of records, and disclosure of payment information of customers which violates PCI-DSS.

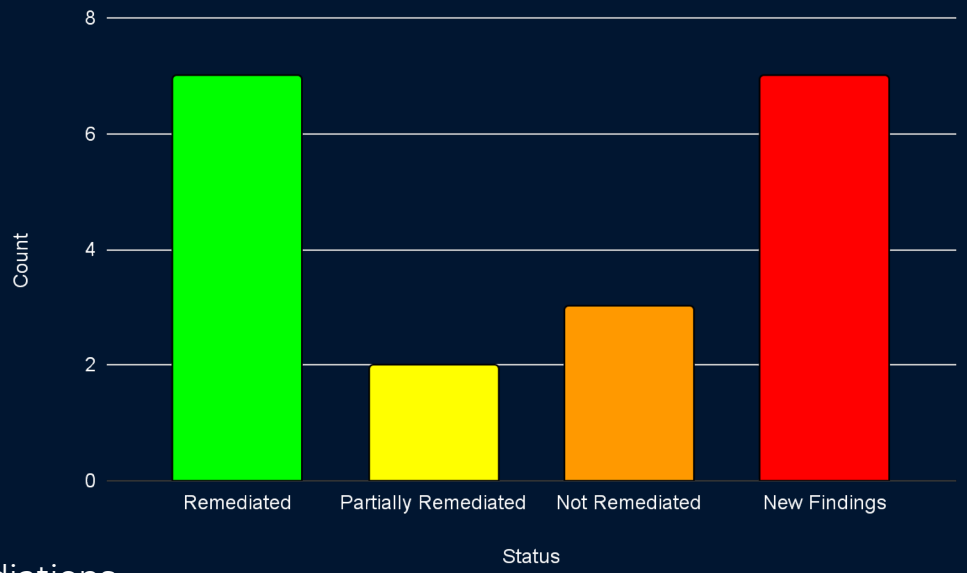
Key Findings

Password Reuse of Compromised Password		CVSS SCORE	PRIORITIZATION
Risk	Critical	7.5 High	CAT-4
Impact	Very High		
Likelihood	Very High		

Description

The host system of 10.0.0.200 maintains various information regarding payments, bookings and reservations, and customer information. Attackers will often reuse compromised passwords as administrators and users don't always change their passwords. Absolute breach of customer privacy is proven in this vulnerability where adversaries are able to view private information about customers. Overall, this results in leak in various data which can result in PCI-DSS violations, fines, as well as legal complications and irreparable reputational damage.

Remediation Assessment



- Remediations
- Partial Remediations
- Not Remediated
- Vulnerabilities

Final-XX observed improved security stature since the last engagement, especially in network security and anti-scanning measures. However,

There is still a long way to go

Compliance & Business Impact

The main purpose of a business is to earn

Profits

This is not possible if you face the wrath non-compliance with standards and regulations

PCI Non-compliance result in fines of upto

$500,000

Consequences of Non-compliance

In addition to:

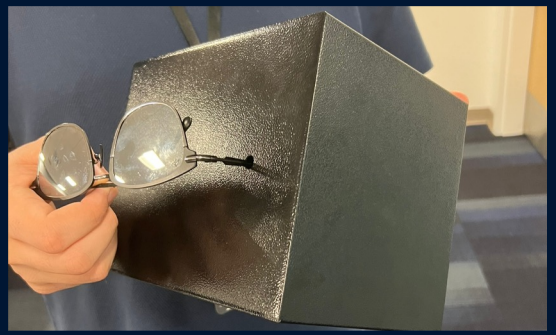
> Increased Audit Requirements

> Extreme reputational damage and mistrust

> Legal consequences due to breaches

> Campus wide shutdown for credit card activity

Physical Assessments of Safes



Remediations and strategic recommendations

1 - Password policy change

2 - Improved segregation of development and production

3 - System Redundancy

4 - Improved data protection and handling of customer data

THANKS!

Do you have any questions?

Finals-XX