Security Assessment Briefing

Le BonBon Croissant

Team XX

Overview

1. The Team
2. Importance of Cybersecurity
3. Assessment Overview
4. Key Findings
5. Strategic Recommendations
6. Compliance
7. Questions

The Team

Importance of Cybersecurity

LE BONBON CROISSANT
CPTC 2021

Risk Classification

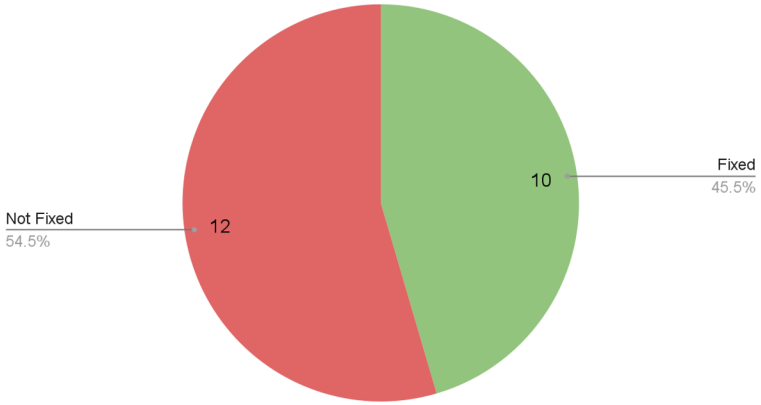
- Severe (> 2
- High (15
- Moderate (10 - 14)
- Low (5 -
- Minimal (< 5

	1- Negligible *Insignificant disruption to operations. Or disruption of less than 2 hours.*	**2 - Minor** *Minimal disruption to operations. Or between 2 and 5 hours of disruption.*	**3 - Moderate** *Noticeable disruption to operations. Or between 5 and 10 hours of disruption.*	**4 - Major** *Operations are severely impacted. Or between and 24 hours of disruption.*	**5 - Catastrophic** *Operations are completed halted or multiple days of disruption*
5 - Very Likely *Above 80% chance of exploitation. Or would require no-skill to exploit.*	5	10	15	20	25
4 - Likely *Between 79% and 60% chance of exploitation. Or would require minimal skill to exploit.*	4	8	12	16	20
3 - Moderate *Between 59% and 30% chance of exploitation. Or would require some skill to exploit.*	3	6	9	12	15
2- Unlikely *Between 29% and 10% chance of exploitation. Or would require expert skills to exploit.*	2	4	6	8	10
1 - Incidental *Less than a 9% change of exploitation. Would only be exploited through accidental means*	1	2	3	4	5

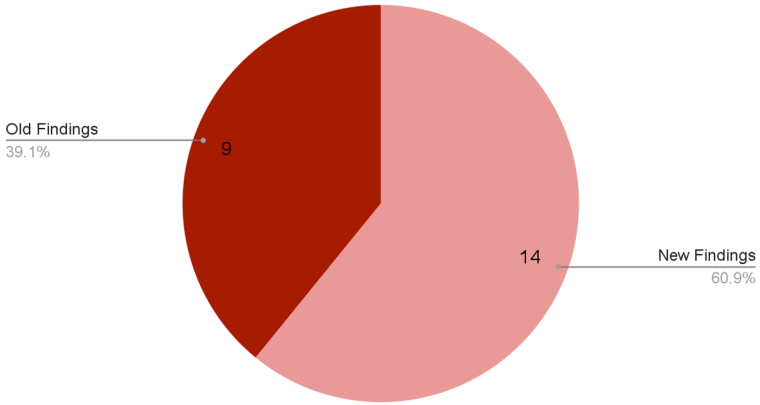
Assessment Summary

- Overall Risk: **Severe**

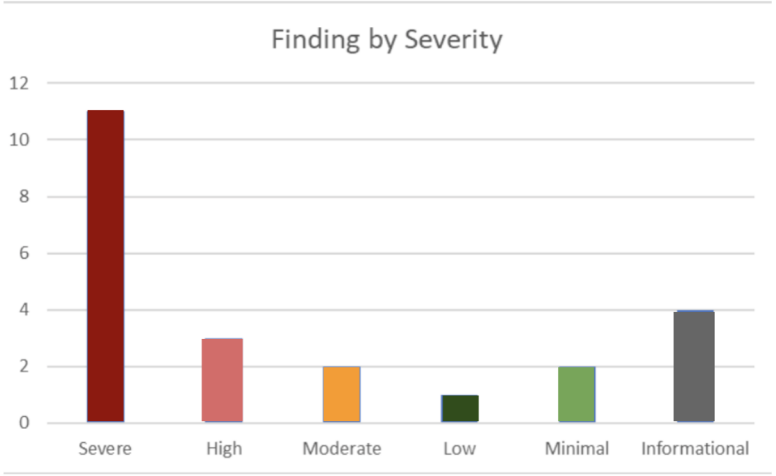
Security Improvements

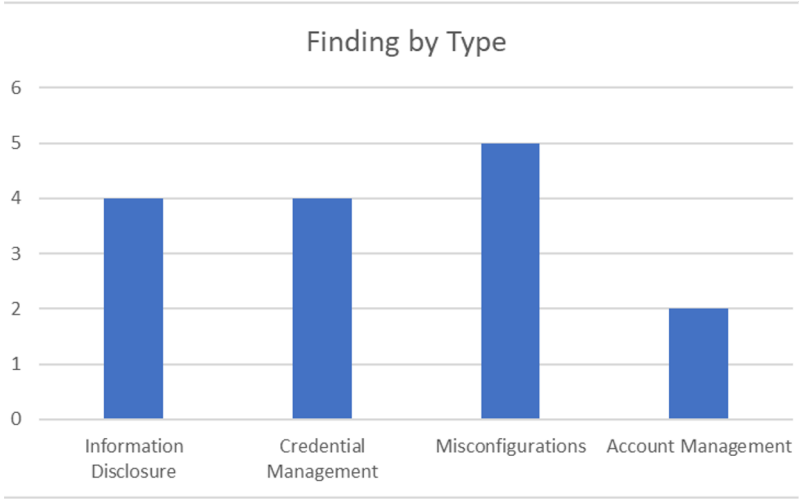


Vulnerability Findings



Assessment Statistics





Key Findings

Credential Issues

Credentials were reused.

Weak credentials were found.

Some hosts allowed unauthenticated access.

Payment Manipulation

A host allowed unauthenticated users to manipulate payment transactions.

Insecure Storage

Sensitive information was often stored unencrypted.

Strategic Recommendations

Strict Password Policy

Passwords should be unique and not reused.

Should be 8 characters long with no repeated characters.

Added two-step login with text code or application such as Duo or Okta.

Encryption

Sensitive client information should be encrypted.

Separate Network

Seperate devices by purpose.

Remove internet access from sensitive devices.

Account Management

Separate access control based on job requirements.

Give each user the least amount of privilege possible.

Compliance

- Payment Card Industry Data Security Standard (PCI-DSS)
    - Fines: **Up to $500,000** per incident
    - Example:
        - Unsecured Credit Card Data Storage
- Global Data Protection Regulation (GDPR)
    - Fines: **20 million euros** or 4% of the company's revenue
    - Example:
        - Data Leakage: Customer Information

Questions?

Contact Information:

finals-xx@cptc.team