A picture containing polygon

Description automatically generated

THE COZY CROISSANT

Security Assessment Findings Report

Business Confidential

Date: November 18, 2022

Project: TCC22

Version 1.0

Table of Contents

[**Confidentiality Statement**](#_heading=h.gjdgxs) **3**

[**Disclaimer**](#_heading=h.30j0zll) **3**

[**Contact Information**](#_heading=h.1fob9te) **4**

[**Assessment Overview**](#_heading=h.3znysh7) **5**

[**Assessment Components**](#_heading=h.2et92p0) **6**

[Internal Penetration Test](#_heading=h.tyjcwt) 6

[**Finding Severity Ratings**](#_heading=h.3dy6vkm) **6**

[**Risk Factors**](#_heading=h.1t3h5sf) **7**

[Likelihood](#_heading=h.4d34og8) 7

[Impact](#_heading=h.17dp8vu) 7

[**Scope**](#_heading=h.3rdcrjn) **7**

[Scope Exclusions](#_heading=h.26in1rg) 7

[Client Allowances](#_heading=h.lnxbz9) 7

[**Executive Summary**](#_heading=h.35nkun2) **7**

[**Vulnerability Report Card**](#_heading=h.1ksv4uv) **8**

[**Vulnerability Summary**](#_heading=h.44sinio) **8**

[**Technical Findings**](#_heading=h.2jxsxqh) **9**

[Finding TCC001: [CVE -] Vulnerability Name](#_heading=h.z337ya) 9

# Confidentiality Statement

This document is the property of The Cozy Croissant and Southeast-2. This document contains sensitive information including proprietary and confidential information. This document shall not be distributed outside of The Cozy Croissant or the Southeast-2 without the express consent of both parties involved.

# Disclaimer

This document contains information regarding the overall network and system security of the Cozy Croissant. While Southeast-2 maintains the highest standards of quality in their work, this document should not be construed as an exhaustive list of all possible vulnerabilities. We have intentionally focused on the areas with the highest risk and greatest vulnerability to attack to maximize the value of our services.

Due to the changing nature of the computer systems and networks, security vulnerabilities and risks will change over time; Southeast-2 recommends annual testing to maintain a good security posture in response to evolving threats.

# Assessment Overview

On November 19th, 2022, Southeast-2 conducted a penetration test to evaluate the overall security posture of the Cozy Croissant. This test was conducted in accordance with industry standard best practices. The phases of the penetration test are as follows:

* Planning – Customer expectations and rules of engagement are obtained.
* Enumeration – Open-source intelligence, and scanning are done to identify common vulnerabilities and weak areas.
* Exploitation – Confirm vulnerabilities by successfully completing an exploit and then perform more discovery based on new information.
* Reporting – Record all vulnerabilities, findings, successful exploits, and organization strengths and weaknesses.









# Assessment Components

## Internal Penetration Test

The internal penetration test will simulate how an attacker would operate inside of the internal network. One member of the team will enumerate the network for vulnerabilities as well as carry out internal network attacks, such as: kerberoasting, token impersonation, pass-the-hash, golden ticket, web exploitations and more. The team member will gain access to hosts through these exploits. They will move through the network using lateral movement eventually attempting to gain access to the domain controller and domain admin accounts.

# Finding Severity Ratings

This section is used to define the severity ratings for any vulnerabilities and measure risk impact. The severity ratings will follow the corresponding CVSS score range.

| Severity | CVSS V3 Score Range | Definition |
| --- | --- | --- |
| Critical | 9.0 – 10.0 | Straightforward exploitation typically results in high level system access. Vulnerabilities of this category should be resolved immediately |
| High | 7.0 – 8.0 | Exploitation may involve more steps but could result in gaining elevated privileges and potentially significant downtime or data loss. Vulnerabilities of this category should be resolved as soon as possible. |
| Medium | 4.0 – 6.9 | Vulnerabilities are present but are not exploitable, involve many extra steps, and/or require social engineering. Vulnerabilities of this category should be resolved after high-priority issues are resolved. |
| Low | 0.1 – 3.9 | Vulnerabilities may be present but are not exploitable. Resolving these vulnerabilities would help to reduce the organization’s attack surface. Vulnerabilities of this category should be resolved during the next period of planned maintenance. |
| Informational | N/A | No vulnerability exists. This category is reserved for findings that do not directly relate to exploitation but may provide an attacker with information that would assist them in an attack. |

# Risk Factors

Risk is measured by two factors: Likelihood and Impact.

## Likelihood

Likelihood measures the probability of a vulnerability being exploited. Severity ratings are used for scoring based on how difficult the attack was, the tools available, skill level of the attacker, and the environment of the client.

## Impact

Impact measures the probability of the vulnerability having an effect on operations in the corporation. This includes the confidentiality, integrity, and availability of client-side systems and data, harm to software and/or hardware, and financial loss.

# Scope

| Assessment | Details |
| --- | --- |
| Corporate Network | 10.0.0.0/24 |
| Guest Network | 10.200.200.0/24 |

## Scope Exclusions

Anything that is explicitly out of scope

The team will not conduct any testing on any externally facing systems or IP addresses. No disruptive or destructive testing will be allowed on any systems.

Testing will be limited to the assigned subnets; the VPN and Pentest box(es) are out of scope.

## Client Allowances

Anything that the client gives us for access

The client will provide a Windows and Kali system for each tester; these will be used as an entry point to other systems.

# Executive Summary

Very brief summary covering the following information: whose security we were evaluating, the date(s) of the evaluation, and what is to follow in the coming sections. Do not need to summarize every section necessarily, just set the expectation of what follows.

# 

# Vulnerability Report Card

| Critical | High | Medium | Low | Informational |
| --- | --- | --- | --- | --- |
| 15 | 32 | 5 | 55 | 21 |

# Vulnerability Summary

| Severity | Vulnerability | Recommendation |
| --- | --- | --- |
| Critical | **TCC001:** XMLRPC Remote Code Execution | Update CMS to latest release |
| High | **TCC002**: Cross site scripting on forum page | Implement input sanitization against user-generated content |
| Medium | **TCC004:** XMLRPC Denial of Service | Update CMS to latest release |
| Low | **TCC006**: Clickjacking against user registration page | Add the ‘X-Frame-Options’ header to site requests and only allow page embeds from the same origin |
| Info | **TCC003**: Regex deficiency in sign up page – does not allow email addresses with capital letters | Review the email matching regex and ensure it includes capital letter matching |

# Technical Findings

## Finding TCC001: [CVE -] Vulnerability Name

| **Affected Hosts** | <Target/affected system> |
| --- | --- |
| **CVSS:** <score> | <rating> | **Likelihood:**  <notes about likelihood of exploitation (difficulty, creds needed, etc.>  **Risk:**  <notes about risk/weaponization potential> |
| **Vulnerability Description** | <describe generally how the vulnerability works and what it allows an attacker to do> |
| **Requirements to exploit** | <include things like tools, creds needed, internal access, etc.> |
| **Remediation** | <general remediation specific to this instance of the exploit. Don’t do IT’s job for them though> |
| **References** |  |

Proof of Concept:

Text

Description automatically generated

A picture containing polygon

Description automatically generated

**Last Page**