

**{{ client.name }}**

**Security Assessment Report**

|  |  |  |
| --- | --- | --- |
| **PREPARED BY** | **DATE** | **VERSION** |
| Central-8 | {{ project.start\_date }} | Version 1.0 |

***Notice of Confidentiality***: This document is confidential and solely intended for OuiCroissant. Unauthorized access, viewing, or distribution of this document is prohibited and may be a violation of federal and state laws, including but not limited to the Defend Trade Secrets Act (DTSA) and the Computer Fraud and Abuse Act (CFAA). Unauthorized individuals found in possession of or distributing this document may be subject to legal action.

***Disclaimer of Warranty and Limitation of Liability***: This report is intended solely for the purpose of assessing the security posture and data compliance status of OuiCroissant. The findings, recommendations, and information contained within this document are provided to assist in identifying potential vulnerabilities and risks within the current operational framework. This document is not a comprehensive guarantee of immunity from future security incidents, data breaches, or other threats. Central-8 provides no assurance, warranty, or representation that the implementation of the recommendations provided will prevent or fully mitigate any and all forms of potential losses, damages, and/or liabilities.

TABLE OF CONTENT GOES HERE

WE CANT REALLY USE IT BECAUSE JINJA TEMPLATING BREAKS IT…

WE DO IT POST.

# Introduction

This penetration testing report provides a comprehensive assessment of the current security posture of Flakebook’s IT infrastructure as of **November 2, 2024**. Penetration tests are a “snapshot in time” and as such, this report offers insights into potential security and operational risks based on existing configurations, network structures, and deployed defenses during the period of this engagement. Because network environments and threat landscapes continuously evolve, this assessment reflects findings only observed at the time of testing. Regular, periodic testing is advised to maintain an up-to-date understanding of security risks.

This report is organized to support both executive decision-making and technical teams in understanding Flakebook and OuiCroissant’s risk profile and in prioritizing strategic remediation efforts. The key sections of this report include:

* ***Executive Summary***: Provides stakeholders with a high-level overview of the penetration test findings, highlighting critical vulnerabilities and their implications. It summarizes the organization’s current security posture and presents essential recommendations to improve defenses and align with organizational goals.
* ***Strategic Plan***: Highlights key security strengths and areas of improvements, as well as providing prioritized recommendations for addressing identified vulnerabilities and improving the organization’s security resilience. This includes both immediate, high-impact mitigations and long-term strategies for enhancing overall security posture and maturity.
* ***Compliance Review***: Evaluates the organization’s alignment with relevant regulatory standards and compliance frameworks, detailing areas where current practices meet, exceed, or fall short of specified requirements.
* ***Engagement Outline***: Describes the overall engagement, including the methodology employed, scope of the assessment, objectives, and timelines established for the engagement.
* ***Severity and Risk Level Classifications***: Explanation of Central-8 scoring metrics used to categorize vulnerabilities based on severity and associated risk levels is provided.
* ***Technical Findings***: Detailed account of the identified vulnerabilities, including their potential impact and risk ratings. Each finding includes technical details and actionable remediation steps, with vulnerabilities ranked by severity to streamline prioritization efforts.

## Contact Information

|  |  |  |
| --- | --- | --- |
| **Organization** | **Point of Contact** | **Contact Information** |
| OuiCroissant | Jamie Thompson | [jthompson@ouicroissant.com](mailto:jthompson@ouicroissant.com)  [secops@ouicroissant.com](mailto:secops@ouicroissant.com) |
| Central-8 | Central-8 | [cptc10-us-central-8@cptc.team](mailto:mailto:cptc10-us-central-8@cptc.team) |

# Executive Overview

## Executive Summary

During the limited assessment period, Central-8 identified 30 unique vulnerabilities across critical, high, medium, and low severity categories. Notably, several critical findings with low attack complexity posed a risk of exposing both employee and customer data from the production network. These vulnerabilities present significant risks to Flakebook and OuiCroissant, including potential data loss, erosion of consumer and employee trust, revenue impacts, and legal liabilities resulting from inadequate security measures.

In addition to identifying vulnerabilities, this report highlights key security strengths within the organization, as well as areas for improvement. Understanding these strengths will enable OuiCroissant and Flakebook as a platform to build upon existing security measures while addressing identified weaknesses. The "Remediation Roadmap" section outlines both short-term and long-term remediation actions aimed at enhancing the overall security posture. These actions are designed to provide a structured approach to mitigating risks and ensuring compliance with security best practices.

Please note that due to the assessment's limited timeframe and the evolving nature of information security, additional vulnerabilities may exist. Ongoing assessments are essential to maintaining a robust and proactive security posture.

|  |  |  |  |
| --- | --- | --- | --- |
| **LOW** | **MEDIUM** | **HIGH** | **CRITICAL** |
| **{{ findings|filter\_severity(["Low"])|length }}** | **{{ findings|filter\_severity(["Medium"])|length }}** | **{{ findings|filter\_severity(["High"])|length }}** | **{{ findings|filter\_severity(["Critical"])|length }}** |

## Key Security Strengths

Throughout the engagement, Central-8 noticed one key strength implemented in OuiCroissant’s organization.

### Security Awareness Training

Central-8 performed three (3) phishing attacks against OuiCroissant employees, and the users did not appear to interact with the emails. This signifies that OuiCroissant maintains good security awareness training to teach employees about cybersecurity risks and best practices.

## Key Security Improvements

Among the 30 unique vulnerabilities identified, Central-8 noticed common themes and patterns. These areas represent key security improvements and implementation of these improvements will be vital to the improving OuiCroissant and Flakebook’s current existing infrastructure, as well as helping stop future vulnerabilities from arising.

### [CWE-653](mailto:https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://cwe.mitre.org/data/definitions/653.html&ved=2ahUKEwjmsvLHob-JAxVkSTABHUlNEu4QFnoECBIQAQ&usg=AOvVaw2vuFdFA_7cI5WRHhpHPoXF): Improper Isolation or Compartmentalization

Flakebook’s internal environment is not isolated, allowing for unnecessary communication between services. Flakebook should adopt an approach of zero-trust architecture to ensure that services can only communicate with services they are required to interact with.

### [CWE-284](mailto:https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://cwe.mitre.org/data/definitions/284.html&ved=2ahUKEwjknv6bob-JAxWiaDABHW9hOkUQFnoECBMQAQ&usg=AOvVaw15x34oI7XbXd-CkB1DjCx9): Improper Access Control

There were multiple vulnerabilities arising from improper authentication, such as unauthenticated MongoDB, API endpoints, and weak credentials. Strong access control should be in place for all services.

### [CWE-272](mailto:https://cwe.mitre.org/data/definitions/272.html): Least Privilege Violation

Throughout the engagement, several privilege escalation vulnerabilities arose due to lack of implementation of the principle of least privilege. OuiCroussant should ensure that users only have the necessary permissions to perform tasks used in their day-to-day operations.

# Remediation roadmap

The following road map has been created by Central-8 to provide OuiCroissant with a timeline by which to plan and execute recommended remediations related to found and exploitable vulnerabilities present in Flakebook. Please note: Central-8 has a limited view into the backend of OuiCroissant and can only offer suggestions based on its prior experiences and findings during the assessment. All remediation recommendations are to be interpreted by qualified professionals with experience working with Flakebooks backend systems. Further technical details to remediation can be found in the Remediation section of each technical finding table.

**1-2 Month**

**6 Mo. – 1Yr**

* **Deploy host-based endpoint defense solutions**: Implement robust antivirus and endpoint detection and response (EDR) products across all hosts to proactively identify, isolate, and remediate threats, ensuring comprehensive protection against malware and advanced cyber threats.
* **Implement Multi-Factor Authentication (MFA):** Enforce MFA across all user accounts and sensitive systems to enhance security, requiring users to provide multiple verification methods – such as passwords, biometrics, or one-time codes – before granting access, thereby reducing the risk of unauthorized access.
* **Implement Network Segmentation:** Implement strategic network segmentation to isolate sensitive data and critical systems, enhancing security by limiting lateral movement within the network. This approach minimizes the attack surface and helps contain potential breaches by creating distinct zones for different types of traffic and user access.
* **Deploy host-based firewall solutions**: Configure comprehensive inbound and outbound rules to safeguard each host in the network, ensuring robust protection against unauthorized access and malicious traffic.
* **Establish secure lockout policies**: Implement stringent account lockout protocols on every host within the network/domain to mitigate the risk of brute force attacks and unauthorized access.
* **Enforce secure password policies**: Apply strong password policies across all hosts in the network/domain, including complexity requirements and regular expiration, to enhance overall security posture.
* **Regularly update and patch systems**: Establish a systematic process for applying updates and security patches to all software, operating systems, and applications. This proactive measure ensures vulnerabilities are promptly addressed, reducing the risk of exploitation and maintaining the integrity of the network.

**Immediate**

# Compliance Review

Flakebook will engage with various regulations in which this section highlights, to follow compliance and ensure privacy. This enforcement is crucial to protecting user data, mitigating legal risks, and safeguarding Flakebook’s reputation as a company. Central-8 brings attention to these compliance regulations from a security perspective as retrospection. In the column labelled “Y/N”, red will represent the requirements found violated, green will represent the requirements that Central-8 accepted as passing compliance, and grey will represent the requirements that were not within scope or were not found during testing. Flakebook is highly encouraged to take consultation with qualified experts, alongside comprehensive audits over company practices and policies.

## General Data Protection Regulation

Flakebook’s global reach as a social media platform will include citizens within the European Union. As a service provider, the company is required to follow the General Data Protection Regulation (GDPR), designed by the European Union to protect the privacy and personal data of its citizens. Any websites in which data is collected and violates compliance, can result in financial penalties, damage to customer trust, and loss of reputation.

### 1Compliance with GDPR

|  |  |  |
| --- | --- | --- |
| **Y/N** | **Reference** | **Requirement** |
| **No** | 25.1 | Data protection by design: Implementation of appropriate technical and organizational measures (such as pseudonymization) designed to implement data-protection principles (data minimization) in an effective manner |
| **No** | 25.2 | Data protection by default: Implementation of appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed |
| **No** | 28.3(c) | When engaging a processor, ensure they take all security measures required pursuant to Article 32 |
| **Unfound** | 29 | Ensure that any person acting under the authority of the controller or processor who has access to personal data processes those data only on instructions from the controller |
| **Unfound** | 30.1(g) | Where possible, include a general description of the technical and organizational security measures referred to in Article 32(1) |
| **No** | 32.1(a) | The controller and processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including pseudonymization and encryption of personal data |
| **No** | 32.1(b) | The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services |
| **Unfound** | 32.1(c) | The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident |
| **Yes** | 32.1(d) | A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing |
| **No** | 32.2 | In assessing the appropriate level of security, account shall be taken in particular of the risks presented by the processing, particularly from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data |
| **Unfound** | 32.4 | Take steps to ensure that any natural person acting under the authority of the controller or processor who has access to personal data does not process them except on instructions from the controller |
| **Does Not Apply** | 33.1 | In the case of a personal data breach, notify the supervisory authority not later than 72 hours after having become aware of it |
| **DNA** | 33.2 | Processor shall notify the controller without undue delay after becoming aware of a personal data breach |
| **DNA** | 33.3 | Document any personal data breaches, including the facts relating to the breach, its effects and the remedial action taken |
| **DNA** | 35.1 | Where processing is likely to result in a high risk, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data |
| **DNA** | 35.7(d) | Include in the Data Protection Impact Assessment (DPIA) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data |

1https://gdpr-info.eu/

## California Consumer Privacy Act

Flakebook’s user base also requires compliance to the California Consumer Privacy Act (CCPA), where residents of the state are given rights regarding personal information. Businesses are to be transparent about data collection under the CCPA and must provide users the ability to access and delete their personal data as well as deny the selling of their information. Non-compliance can result in fines, legal repercussions, damaged reputation, and loss in user trust.

### 2Compliance with CCPA

|  |  |  |
| --- | --- | --- |
| **Y/N** | **Reference** | **Requirement** |
| **No** | 1798.81.5(a) | Implement and maintain reasonable security procedures and practices in protecting personal information from unauthorized access, destruction, use, modification, or disclosure |
| **No** | 1798.81.5(b) | A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information |
| **Yes** | 1798.81.5(c) | Contractually require third parties with access to personal information to implement and maintain reasonable security procedures |
| **No** | 1798.100(e) | Implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure |
| **Unfound** | 1798.130(a)(5) | Use reasonable security measures when transmitting personal information to the consumer |
| **Unfound** | 1798.140(ag) | If sharing personal information with a third party or service provider, enter into a contractual agreement that obligates them to provide the same level of privacy protection as required by CCPA |
| **Unfound** | 1798.145(m) | Cooperate with law enforcement regarding data breaches or other security incidents |
| **No** | 1798.150(a)(1) | Implement and maintain reasonable security procedures and practices to protect consumer's nonencrypted and nonredacted personal information from unauthorized access, exfiltration, theft, or disclosure |
| **Yes** | 1798.185(a)(15)(A) | Perform annual cybersecurity audits if processing presents significant risk to consumers' privacy or security |
| **DNA** | 1798.185(a)(15)(B) | Submit regular risk assessments to the California Privacy Protection Agency of processing activities that present significant risk to consumers' privacy or security |

2https://oag.ca.gov/privacy/ccpa

## Children’s Online Privacy Protection Act

Due to Flakebook not containing age validation, the company is subject to the Children’s Online Privacy Protection Act (COPPA), created to protect users under the age of 13. COPPA imposes specific requirements regarding the collection, use, and disclosure of children’s personal information. Violations of the federal law can result in significant financial penalties, varying legal action, critical damage to the credibility of the platform, and the loss of parental trust.

### 3Compliance with COPPA

|  |  |  |
| --- | --- | --- |
| **Y/N** | **Reference** | **Requirement** |
| **No** | 312.3(e) | Establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children |
| **No** | 312.4(d) | Implement reasonable technical measures to maintain security of direct notices to parents |
| **No** | 312.5(c)(1) | Use reasonable technical measures to ensure that the person providing consent is the child's parent when using email-plus verification |
| **No** | 312.8 | Operators must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children. The operator must also take reasonable steps to release children's personal information only to service providers and third parties who are capable of maintaining the confidentiality, security, and integrity of such information, and who provide assurances that they will maintain the information in such a manner |

3https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa

# Engagement Outline

## Methodology

To ensure consistent and standardized results, the Penetration Testing Execution Standard (PTES), is used by Central-8. This approach not only facilitates transparent communication during the pre-engagement phase but also ensures a thorough and all-encompassing assessment. Many regulatory frameworks and industry standards require or recommend penetration tests and using a standardized framework like PTES can help organizations demonstrate compliance with these requirements. Additionally, following standardized approaches allows future and past tests to be benchmarked, to see improvements or regressions, if any.

* ***Pre-Engagement Interactions*:** Scoping, Rules of Engagement, etc.
* ***Intelligence Gathering*:** Aims to gain information about Flakebook.
* ***Threat Modeling*:** Models potential threats and vulnerabilities specific to Flakebook.
* ***Vulnerability Analysis*:** Analyze potential threats for vulnerabilities.
* ***Exploitation*:** Exploit found vulnerabilities to gain initial access to systems
* ***Post Exploitation*:** Attempt to move laterally within the network to gain further access.
* ***Reporting*:** Summarize findings and provide actionable recommendations.

## Network Diagram

A screenshot of a computer

Description automatically generated

## Scope

The scope of this test consisted of the production subnet (10.0.1.0/24) and the development subnet (10.0.2.0/24) within the Flakebook network. The entirety of this engagement was performed with the intention of the limited-scope subnet remaining available and functional. If modifications in reference to sensitive data and physical machines were changed through the process, all instructions to reset or revert such actions will be given within indicators of compromise (IOC) section within *Appendix D*, subsection: *Indicators of Compromise*.

## Attack Narrative

Over the course of our assessment, Central-8 found a number of vulnerabilities. With access beginning at 9:00am (central time), within the first hour Central-8 identified a critical configuration vulnerability in the FTP server on the production network allowing anonymous writing to the files stored on the system. On this system we also found a set of hard coded credentials, these credentials would provide access to both windows workstations in the development network. Within the following hour, more hard coded credentials were found in application source code. These would work on the exchange server and provide access to these users personal email client and Microsoft Exchange data. Just before 12:00am, Central-8 was able to break the password hash of a service logon that was obtained through a common enumeration technique known as keurberosting. Using this credential, and the services improper access control Central-8 was able to escalate to administrator credentials on the domain controller, where plaintext/reversibly encrypted passwords are stored and managed, thus resulting in compromises of every single employee account and password on the Windows Active Directory system. While this privilege escalation was occurring, Central-8 also compromised the Postgres database hosted on the Production environment using default credentials left in place during the creation of the database. This access would allow Central-8 to dump and exfiltrate the entire contents of the database including plaintext usernames, passwords, and hashes of Flakebook customers. Additionally, posts, comments, emojis, reactions, and authentication attempts were all contained in this database and were compromised as a result. Later on within the exercise unauthenticated access to a MongoDB instance within the network was obtained. Lastly the Central-8 launched a phishing campaign on three separate targets within the Flakebook network. Our campaign was not fruitful indicating a strong focus on employee awareness within the company.

# Technical Risk Assessment Metrics

Central-8 categorizes findings using a combination of *severity* and *risk*. For severity, Central-8 utilizes the Common Vulnerability Scoring System (CVSSv3) to determine the severity of identified vulnerabilities. CVSS allows vulnerabilities in different applications and from different vendors to be evaluated in a standardized and repeatable way. While CVSS effectively measures severity, it is important to note, as the National Institute of Standards and Technology (NIST) explicitly states that “CVSS is not a measure of risk.”

To address this gap, Central-8 combines CVSS with a modified version of the NIST SP-800-30 risk matrix to calculate a risk score. Risk-based testing considers the unique context of the organization and prioritizes vulnerabilities based on their potential impact on the business. This approach considers assets and likelihood of a successful attack.

By evaluating both the potential impact and the likelihood of a successful exploit, this approach ensures that security efforts are directed towards mitigating the most significant threats -- those that are not only highly impactful but also likely to materialize.

|  |  |
| --- | --- |
| **SEVERITY SCORE** | |
| 0.00 | NONE |
| 0.1 – 3.9 | LOW |
| 4.0 – 6.9 | MEDIUM |
| 7.0 – 8.9 | HIGH |
| 9.0 – 10.0 | CRITICAL |

*CVSSv3 scoring table used to determine vulnerability*

*severity*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **RISK LEVEL** | | LIKELIHOOD LEVEL | | | |
| NONE/LOW | MEDIUM | HIGH | CRITICAL |
| IMPACT LEVEL | NONE/LOW |  |  |  |  |
| MEDIUM |  |  |  |  |
| HIGH |  |  |  |  |
| CRITICAL |  |  |  |  |

*Central-8’s modified NIST SP-800-30 risk matrix to*

*calculate Risk Level based on likelihood and impact*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **OVERALL SCORE** | | SEVERITY LEVEL | | | |
| NONE/LOW | MEDIUM | HIGH | CRITICAL |
| RISK LEVEL | NONE/LOW |  |  |  |  |
| MEDIUM |  |  |  |  |
| HIGH |  |  |  |  |
| CRITICAL |  |  |  |  |

*Central-8’s overall scoring matrix to calculate vulnerability*

*score based on risk and severity*

# Technical Findings

## Critical Findings

{% for finding in findings|filter\_severity([“Critical”]) %}

### {{ finding.title }}

**Overview**: {{ finding.extra\_fields.overview }}

|  |  |  |  |
| --- | --- | --- | --- |
| {{ finding.title }} | | CVSS | Risk |
| Impact | {{ finding.extra\_fields.impact }} | **{{ finding.cvss\_score }}** | **{{ finding.** **extra\_fields. risk }}** |
| Likelihood | {{ finding.extra\_fields.likelihood }} |
| CVSS String | {{ finding.cvss\_vector }} | | |
| Affected Scope | {{p finding.extra\_fields.scope }} | | |
| Summary | {{p finding.extra\_fields.summary }} | | |
| Technical Impact | {{p finding.extra\_fields.technical\_impact }} | | |
| Business Impact | {{p finding.extra\_fields.business\_impact }} | | |
| Likelihood Description | {{p finding.extra\_fields.likelihood\_description }} | | |
| MITRE ATT&CK | {{p finding.extra\_fields.mitre }} | | |
| Compliance Violations | {{p finding.extra\_fields.compliance }} | | |
| Evidence | | | |
| {{p finding.extra\_fields.evidence }} | | | |
| Remediation | | | |
| {{p finding.extra\_fields.remediation }} | | | |

***END OF FINDING BLOCK***

{% endfor %}

## High Findings

{% for finding in findings|filter\_severity([“High”]) %}

### {{ finding.title }}

**Overview**: {{ finding.extra\_fields.overview }}

|  |  |  |  |
| --- | --- | --- | --- |
| {{ finding.title }} | | CVSS | Risk |
| Impact | {{ finding.extra\_fields.impact }} | **{{ finding.cvss\_score }}** | **{{ finding.** **extra\_fields. risk }}** |
| Likelihood | {{ finding.extra\_fields.likelihood }} |
| CVSS String | {{ finding.cvss\_vector }} | | |
| Affected Scope | {{p finding.extra\_fields.scope }} | | |
| Summary | {{p finding.extra\_fields.summary }} | | |
| Technical Impact | {{p finding.extra\_fields.technical\_impact }} | | |
| Business Impact | {{p finding.extra\_fields.business\_impact }} | | |
| Likelihood Description | {{p finding.extra\_fields.likelihood\_description }} | | |
| MITRE ATT&CK | {{p finding.extra\_fields.mitre }} | | |
| Compliance Violations | {{p finding.extra\_fields.compliance }} | | |
| Evidence | | | |
| {{p finding.extra\_fields.evidence }} | | | |
| Remediation | | | |
| {{p finding.extra\_fields.remediation }} | | | |

***END OF FINDING BLOCK***

{% endfor %}

## Medium Findings

{% for finding in findings|filter\_severity([“Medium”]) %}

### {{ finding.title }}

**Overview**: {{ finding.extra\_fields.overview }}

|  |  |  |  |
| --- | --- | --- | --- |
| {{ finding.title }} | | CVSS | Risk |
| Impact | {{ finding.extra\_fields.impact }} | **{{ finding.cvss\_score }}** | **{{ finding.** **extra\_fields. risk }}** |
| Likelihood | {{ finding.extra\_fields.likelihood }} |
| CVSS String | {{ finding.cvss\_vector }} | | |
| Affected Scope | {{p finding.extra\_fields.scope }} | | |
| Summary | {{p finding.extra\_fields.summary }} | | |
| Technical Impact | {{p finding.extra\_fields.technical\_impact }} | | |
| Business Impact | {{p finding.extra\_fields.business\_impact }} | | |
| Likelihood Description | {{p finding.extra\_fields.likelihood\_description }} | | |
| MITRE ATT&CK | {{p finding.extra\_fields.mitre }} | | |
| Compliance Violations | {{p finding.extra\_fields.compliance }} | | |
| Evidence | | | |
| {{p finding.extra\_fields.evidence }} | | | |
| Remediation | | | |
| {{p finding.extra\_fields.remediation }} | | | |

***END OF FINDING BLOCK***

{% endfor %}

## Low Findings

{% for finding in findings|filter\_severity([“Low”]) %}

### {{ finding.title }}

**Overview**: {{ finding.extra\_fields.overview }}

|  |  |  |  |
| --- | --- | --- | --- |
| {{ finding.title }} | | CVSS | Risk |
| Impact | {{ finding.extra\_fields.impact }} | **{{ finding.cvss\_score }}** | **{{ finding.** **extra\_fields. risk }}** |
| Likelihood | {{ finding.extra\_fields.likelihood }} |
| CVSS String | {{ finding.cvss\_vector }} | | |
| Affected Scope | {{p finding.extra\_fields.scope }} | | |
| Summary | {{p finding.extra\_fields.summary }} | | |
| Technical Impact | {{p finding.extra\_fields.technical\_impact }} | | |
| Business Impact | {{p finding.extra\_fields.business\_impact }} | | |
| Likelihood Description | {{p finding.extra\_fields.likelihood\_description }} | | |
| MITRE ATT&CK | {{p finding.extra\_fields.mitre }} | | |
| Compliance Violations | {{p finding.extra\_fields.compliance }} | | |
| Evidence | | | |
| {{p finding.extra\_fields.evidence }} | | | |
| Remediation | | | |
| {{p finding.extra\_fields.remediation }} | | | |

***END OF FINDING BLOCK***

{% endfor %}

# Social Engineering Findings

Central-8 was tasked with performing a social engineering attack on three (3) OuiCroissant employees. Social engineering attacks are manipulative tactics used by malicious actors to try and gain sensitive information or perform malicious actions. By performing social engineering attacks as part of the penetration test, Central-8 can test current employee security awareness and find gaps in OuiCroissant’s existing employee security training model.

To perform this test, Central-8 first chose three targets based on their roles within the organization, the likelihood of their interaction with sensitive data, and their previous training participation. We considered employees from the finance, HR, and IT departments, as these areas are often rich in sensitive information. For the subject lines and body content of the emails, we crafted messages that mimicked internal communications. Then, we developed two payloads using *msfvenom*: one for a Windows executable (.exe) and another embedded in a Microsoft Word document (.doc).

Lastly, we utilized *swaks* to send the emails from the Flakemail server (10.0.1.7), ensuring that the headers and content mimicked genuine internal emails to enhance credibility. By analyzing the responses and actions taken by the targets, Central-8 aimed to evaluate the effectiveness of OuiCroissant’s employee security training and identify areas for improvement.

## Social Engineering Attack #1

|  |  |
| --- | --- |
| **TO** | **FROM** |
| Dakota Mitchell [dmitchell@ouicroissant.local](mailto:dmitchell@ouicroissant.local) | Jamie Thompson [jthompson@ouicroissant.local](mailto:jthompson@ouicroissant.local) |
| **SUBJECT** | |
| Security Patches after Recent Pentest | |
| **BODY** | |
| Dear Dakota,  As you may know, we recently underwent an external penetration test. They were able to identify several vulnerabilities across the Flakebook network and we need to push out patches ASAP.  My team has developed a manual hotfix to remediate most of the issues. I’ve attached the hotfix to this email, can you please apply the patch and provide the output log it generates? We want to make sure we get everything secured in a timely manner.  Let me know when you’ve applied the patch and reach out if you have any issues running it.  Thank you,  Jamie Thompson | |

## Social Engineering Attack #2 (OSINT Finding Used)

Note: Here we used information gained from the public social media account of Jamie Thompson to further increase odds of a successful phish. (https://m.facebook.com/61565356478821/)

|  |  |
| --- | --- |
| **TO** | **FROM** |
| Devin Scott [dscott@ouicroissant.local](mailto:dscott@ouicroissant.local) | Jamie Thompson [jthompson@ouicroissant.local](mailto:jthompson@ouicroissant.local) |
| **SUBJECT** | |
| Sensitive Information Disclosure | |
| **BODY** | |
| Dear Devin,    During a routine GDPR compliance audit, we discovered information on social media that correlates to your account password ending in XXXXXXXX0907. Please see the attached document outlining the process to reset your password.    If you have any questions or concerns, reach out to our SecOps team, [secops@ouicroissant.com](mailto:secops@ouicroissant.com).    Thank you,  Jamie Thompson | |

## Social Engineering Attack #3

|  |  |
| --- | --- |
| **TO** | **FROM** |
| Natalie Heath [nheath@ouicroissant.local](mailto:nheath@ouicroissant.local) | Mack Morissey [mmorissey@ouicroissant.local](mailto:mmorissey@ouicroissant.local) |
| **SUBJECT** | |
| Employee Benefits Survey | |
| **BODY** | |
| Dear Natalie,  As we push through Q4, as you know, OuiCroissant is always looking to ensure our employees mental and financial wellbeing. We have put together a Benefits Questionnaire to survey different aspects of our current benefits package such as bonuses, insurance, time off, retirement, and personal well-being. This survey is completely anonymous, but your feedback will be greatly appreciated in ensuring OuiCroissant retains a healthy workplace environment.  Filled out surveys can be sent to benefits@ouicroissant.com.  Regards,  Mack Morissey | |

# Artificial Intelligence Model Evaluation

OuiCroussant requested Central-8 to perform red teaming against their new large language models (LLM) to determine if the model(s) were vulnerable to jailbreaking to expose sensitive information and perform tasks not within scope for the models.

## Password Manager 1 Bypass

The first model (“Password Manager 1”) is tasked with acting as a password manager with limited prompt security. Central-8 was able to extract the credential by querying the model to determine what user had access to the credential.

A screenshot of a computer

Description automatically generated

## Password Manager 2 Bypass

The second model (“Password Manager 2”) is an improved version of the first model with better security in place. Like our attack in Password Manager 1, we were able to query the prompt to determine what requirements were necessary to authenticate to receive the password and exploited those.

A screenshot of a computer

Description automatically generated

## Password Manager 3

Central-8 was unable to manipulate the third model (“Password Manager 3”) into sharing credentials. This model seems to be effective at mitigating jailbreak and prompt injection attacks, but more extensive testing is recommended to ensure there are no gaps in coverage.

## Content Moderation Bypass

The content moderation model is designed to help enforce Flakebook’s user policy against posts containing cats. Central-8 was able to bypass the content moderation filter by using different encodings for “cat”, such as base64.

A screenshot of a computer

Description automatically generated

# Appendices

## Appendix A: Tools

To achieve a thorough penetration test, Central-8 utilizes a wide range of industry-standard tools along with tools developed by Central-8. Central-8 has carefully ensured every tool's functionality and stability to ensure precision during engagements.

### Reconnaissance

|  |  |
| --- | --- |
| **R3CON** | |
| **Description** | **URL** |
| R3CON is a collaborative platform developed by Central-8 to centralize Nmap scans. Central-8 uses R3CON to reduce redundant scans after the reconnaissance phase and organize scan results on a centralized platform. |  |
| **Gobuster** | |
| Gobuster is a tool used to brute-force: directories and files in websites, DNS subdomains, Virtual Host names on target web servers, Open Amazon S3 buckets, Open Google Cloud buckets and TFTP servers. | <https://github.com/OJ/gobuster> |
| **Feroxbuster** | |
| Feroxbuster is used for brute-forcing directories and files using wordlists. | <https://github.com/epi052/feroxbuster> |
| **Autorecon** | |
| Autorecon is a multi-threaded network reconnaissance tool which performs automated enumeration of services. AutoRecon can perform port scans and directory brute forcing. | <https://github.com/Tib3rius/AutoRecon> |
| **Nmap** | |
| Nmap uses raw IP packets to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, and what type of packet filters/firewalls are in use. | <https://nmap.org/> |

### Exploitation

|  |  |
| --- | --- |
| **Metasploit** | |
| **Description** | **URL** |
| Metasploit provides various payloads, exploits, and auxiliary modules to exploit vulnerable versions of services. | <https://github.com/rapid7/metasploit-framework> |
| **Msfvenom** | |
| Msfvenom assists Metasploit in generating and encoding payloads | <https://docs.metasploit.com/docs/using-metasploit/basics/how-to-use-msfvenom.html> |
| **Impacket** | |
| Impacket is a collection of Python classes for working with network protocols. | <https://github.com/forta/impacket> |
| **Swaks** | |
| Swaks is a multi-tool for SMTP testing | <https://github.com/jetmore/swaks> |
| **SQLMap** | |
| SQLMap is an open-source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over database servers. | <https://github.com/sqlmapproject/sqlmap> |
| **NetExec** | |
| NetExec is a network service exploitation tool that helps automate assessing common protocols and services. | <https://github.com/Pennyw0rth/NetExec> |
| **Hydra** | |
| Hydra is a parallelized login cracker which supports numerous protocols to attack and be used for password spraying. | <https://github.com/vanhauser-thc/thc-hydra> |
| **Hashcat** | |
| Hashcat is the world’s fastest and most advanced password recovery utility, supporting five unique modes of attack for over 300 highly optimized hashing algorithms. | <https://hashcat.net/hashcat/> |
| **Rubeus** | |
| Rubeus is a C# toolset for raw Kerberos interation and abuses. It is often used for ASP-REP Roasting attacks. | <https://github.com/GhostPack/Ruebus> |
| **Python Upload Server** | |
| CENTRAL-8 uses a python upload server to upload evidence and tools needed to conduct thorough testing. | <https://pypi.org/project/uploadserver/> |

### Post-Exploitation

|  |  |
| --- | --- |
| **Evil-WinRm** | |
| **Description** | **URL** |
| Evil-WinRM uses Powershell Remoting protocol to remotely login with to systems with credentials, plaintext or hashes. | <https://github.com/Hackplayers/evil-winrm> |
| **ILSpy** | |
| An open-source .NET assembly browser and decompiler. | <https://github.com/icsharpcode/ILSpy> |
| **Bloodhound** | |
| BloodHound uses graph theory to reveal the hidden and often unintended relationships within an Active Directory enviroment. It can identify attack paths within Active Directory. | <https://github.com/BloodHoundAD/BloodHound> |
| **Mimikatz** | |
| Mimikatz is used to extract plaintexts, passwords, hash, PIN code and kerberos tickets from memory. | <https://github.com/ParrotSec/mimikatz> |
| **PEASS-ng** | |
| PEASS-ng is a suite of tools used to search for possible local privilege escalation paths that you could exploit and print them to you with nice colors so you can recognize the misconfigurations easily. | <https://github.com/peass-ng/PEASS-ng> |
| **adPEAS** | |
| adPEAS is a PowerShell tool to automate Active Directory enumeration. Similar to PEASS-ng tools. | <https://github.com/61106960/adPEAS> |
| **Certipy** | |
| Certipy is an offensive tool for enumerating and abusing Active Directory Certificate Services. | <https://github.com/ly4k/Certipy> |
| **PowerUp** | |
| PowerUp targets common Windows privileges escalation vectors that rely on misconfigurations. | <https://github.com/PowerShellMafia/PowerSploit/tree/master/Privesc> |
| **Seatbelt** | |
| Seatbelt is another privilege escalation tool for Windows that checks for misconfigurations. | <https://github.com/GhostPack/Seatbelt> |
| **Ligolo-ng** | |
| Ligolo-ng is a simple, lightweight and fast tool that allows penetration testers to establish tunnels from a reverse TCP/TLS connection using a tun interface. | <https://github.com/nicocha30/ligolo-ng> |

## Appendix B: Finding Block Legend

The following tables explain the criteria for different categories of vulnerability severity, impact, and likelihood; ranging from “Low/None” to “Critical”.

### Severity Level Explanation

|  |  |
| --- | --- |
| **Critical** | Vulnerability poses an immediate and significant threat, capable of causing extensive system compromise. Has the potential to lead to significant data breaches, severe operational disruption, or total system control by attackers. Immediate action is required to mitigate. |
| **High** | Vulnerability could lead to unauthorized access, data manipulation, or a significant reduction in system availability. Exploiting this vulnerability may not lead to full system compromise but can still result in considerable damage, including partial breaches and operational downtime. |
| **Medium** | Vulnerability may allow for limited access or manipulation of data but typically requires chaining with other vulnerabilities to cause significant harm. The issue may affect certain systems or users but does not pose an immediate, widespread threat. Mitigation is necessary, but less urgent compared to critical/high issues. |
| **Low/None** | Vulnerability has minimal impact on the system or data security. Exploitation is unlikely to lead to significant damage or loss, often due to requiring multiple factors to be exploited effectively. These issues are usually more of a nuisance than a real threat but should still be addressed over time. |

### Impact Level Explanation

|  |  |
| --- | --- |
| **Critical** | A breach or exploitation would cause catastrophic operational failure, significant financial loss, severe reputational damage, or major regulatory/legal non-compliance. This impact could potentially result in long-term damage to the organization. |
| **High** | The impact of this vulnerability is considerable, likely leading to substantial financial loss, significant reputational damage, or regulatory penalties. While the organization may recover in a reasonable timeframe, it would face a significant hit in terms of customer trust or operational downtime. |
| **Medium** | The impact of exploitation may lead to moderate financial losses or operational issues. Reputational damage is likely but limited in scope, and regulatory consequences may be avoidable with proper handling. The organization can recover, but will need effort to restore confidence or normal operations. |
| **Low/None** | Exploitation would have minimal effect on operations or reputation. Financial or compliance impact is either negligible or easily mitigated. The organization can continue functioning with little interruption, and damage control is limited. |

### Likelihood Level Explanation

|  |  |
| --- | --- |
| **Critical** | The vulnerability is extremely likely to be exploited in the near term. It is either actively being exploited in the wild or can easily be targeted due to known attack vectors. Exploitation typically requires minimal effort or skill and can have devastating consequences. |
| **High** | The vulnerability has a high chance of being exploited, with a known attack method available. It may not be actively targeted yet, but it is highly attractive to attackers. Exploitation would require only moderate effort or resources, making this a significant risk. |
| **Medium** | The vulnerability could be exploited, but the likelihood is lower due to the complexity of the attack, the need for insider knowledge, or the need for specific conditions. Exploitations may occur but would typically require some advanced skills or extensive access to the system. |
| **Low/None** | The vulnerability is unlikely to be exploited, either because it is difficult to exploit, requires significant expertise, or the attack surface is limited. Exploiting this vulnerability would require extensive resources or knowledge, making it less attractive to most attackers. |

## Appendix C: Network Inventory

|  |  |  |  |
| --- | --- | --- | --- |
| **IP Addr.​** | **Hostname​** | **Ports​** | **OS​** |
| 10.0.1.5​ | **dockercompute.prod.oui.local**​ | 22, 80, 3000, 5000, 5432, 8080, 9999​ | Linux​ |
| 10.0.1.6​ | **flakead.oui.local**​ | 53,80,88,135,139,389,443, 445, 464, 593, 636, 3268, 3289, 3389​ | Windows​ |
| 10.0.1.7​ | **flakemail.oui.local**​ | 25, 80, 81, 110, 135, 139, 143, 443, 444, 445, 465, 587, 593, 808, 993, 995, 2525, 3389, 3800, 3801, 3828, 5060, 6001, 6580, 6969​ | Windows​ |
| 10.0.2.5​ | **dockercompute-dev.dev.oui.local**​ | 22, 80, 443, 5000, 8080​ | Linux​ |
| 10.0.2.100​ | **OC-Desktop01.oui.local**​ | 135, 139, 445, 3389​ | Windows​ |
| 10.0.2.104​ | **OC-Desktop04.oui.local**​ | 135, 139, 445, 2121, 3389​ | Windows​ |
| 10.0.2.250​ | **networkdebug.dev.oui.local**​ | 22​ | Linux​ |

## Appendix D: Artifacts

### Indicators of Compromise (IOC)

* Workstation 1
  + C:\Users\DevAutomation\Downloads\adPEAS.ps1
  + Hash: 2d0467a164b7903e1ab6320f678765eb32b7c80f9260c2e96e95addf6dae00e2
* FlakeAD
  + C:\Windows\Temp\adPEAS.ps1
  + Hash: 2d0467a164b7903e1ab6320f678765eb32b7c80f9260c2e96e95addf6dae00e2
* FlakeAD
  + C:\Windows\Temp\Invoke-MimiKatz.ps1
  + Hash: a07a6ba5eda111901571883b464d8dfe852aec006bf639b1f25b7a51611a4ce9
* FlakeAD
  + C:\Windows\Temp\SharpHound.exe
  + Hash: 1fb71035ee32199280564981c04b6e4ed9e19174e1aac8e9cbe404d47300c362
* FlakeAD
  + Domain admin `kali` added to domain

### Compromised Accounts

* All OuiCroissant Domain users
* All Flakebook customers