THE COZY CROISSANT

PENETRATION TESTING AND RISK ASSESSMENT REPORT

REPORT ISSUED:

[redacted]

January 14, 2023

Table of Contents

Disclosure Statement

This report was prepared by [redacted] at the request of The Cozy Croissant Ltd. All information contained in this document is confidential in accordance with the signed non-disclosure agreement put forth by The Cozy Croissant. It should not be distributed, viewed, published, or otherwise distributed without permission from The Cozy Croissant and [redacted] Given the limited scope and time available for the preparation of the report, it should not be taken as a complete account of security vulnerabilities.

The information contained in this report is provided for informational purposes only. The report is based on a penetration testing engagement that was conducted under controlled conditions and is not intended to reflect the results of a real-world attack. The report should not be used as the sole basis for making security decisions. The report is intended to be used as a tool for identifying potential vulnerabilities in a system. The results of the penetration testing engagement should be used in conjunction with other security measures to ensure the overall security of the system.

Contact Information

[redacted]

Executive summary

Introduction

[redacted] performed an 18-hour penetration test for The Cozy Croissant Ltd. (TCC) on the 13th and 14th of January 2023 to evaluate 1) risk exposure, 2) compliance with regulatory requirements, and 3) updates to its cybersecurity infrastructure since the first wave of penetration tests in [redacted] of 2022.

This report details the technical findings of the penetration test. Vulnerabilities found by our team are given a CCVS threat level, and their potential impact on TCC's business operations is discussed as part of our multidisciplinary approach to cybersecurity solutions. Our penetration testing strategy, as always, prioritized the safety of the client's network. We remained in active communication with TCC's IT team throughout, ensuring that business operations could continue unaffected.

TCC has been hard at work renovating and improving its cybersecurity infrastructure, boasting an active and robust IT team, and many improvements were noted by our team during this penetration test. Noting the fact that the hospitality industry faces some of the highest rates of cybersecurity attacks, we were focused on emulating the behavior of attackers to properly appraise the dangers faced by TCC's network. Our team also took special consideration of TCC's compliance with regulations concerning client information security, be they regional, national or international. Particular attention was directed toward compliance with state-level information security laws, federal COPPA regulations, and international GDPR and PCI-DSS requirements. This is due to the rapid pace of change that has been taking place in this field, and to which TCC should pay attention to moving forward with both its business operations and cybersecurity department.

Overall, a number of highly critical threats, vulnerabilities, and breaches of the regulation still exist within the network and should be remedied urgently; TCC faces a multitude of risks that are addressed at length in the remainder of this report. Firstly, malicious attackers can restrict or deny access to TCC's systems with the aim of compromising client information or launching ransomware attacks constituting a major operational risk. Secondly, TCC faces compliance and reputational risks associated with failing to meet the requirements of important regulations, which could cause the business to lose the trust of its consumers and suppliers, as well as the confidence of staff members. Third, TCC faces the financial risk of fines associated with the aforementioned regulations, as well as lawsuits by clients and staff members protesting poor information security policies. All of these risks gain heightened importance due to TCC's market positioning as a small hotel facing fierce competition from local and international competitors in the form of other hotel chains and Airbnb services.

Despite these challenges, TCC also has access to a large number of opportunities. Cybersecurity practices in the hospitality industry are entering a new period marked by plentiful

access to new technical resources, best practices, and clear protocols tailored to the demands of the industry. The current landmark at the time of publishing is the NIST report "*Securing Property Management Systems*" released in the latter half of 2021, upon which many of the recommendations of this report are based. Information laws have also been advancing at a staggering pace ever since the enforcement of the GDPR in Europe and the CPPA in the United States, and are likely to continue growing in depth and scope as time goes on. TCC is uniquely poised to take advantage of this junction in history, and being an early adopter of these best practices, resources, and regulations could grant the firm a critical leg above the competition and turn them into a pioneer in the field of consumer protection and privacy in the eyes of customers.

[redacted] is delighted to have had this opportunity to work with TCC and certainly looks forward to future cooperation and frequent collaboration with a future leader of the hospitality industry.

Compliance and Regulation in a Changing Business Environment

Representing Croissant Holdings' first foray into the hospitality industry, TCC is likely to face security and IT challenges unique to that field and outside of the accumulated experience of Croissant Holding's team. Due to the nature of their business, TCC requires access to important guest information, some of which can be considered Personally Identifiable Information, bringing with it regulations on consumer privacy and data security.

According to our research, there are three spheres of information laws and regulations affecting TCC: State-level, Federal, and International.

State-level regulations:
The statutes of the state of Nevada discuss relevant information laws under Chapter 603A - Security and Privacy of Personal Information. The provision defines data collectors, personal information, and under what conditions breaches of the security of system data are defined. Subclause A.210 lists necessary security measures that data collectors and businesses must abide by, requiring that they "implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure." In addition, data collectors are required to abide by industry standards as defined by the CIS and NIST. Finally, the provision lists penalties for violating the above requirements, these fall under the penalties for deceptive trade practices, and include fines of up to $12,500 per violation.

Federal Regulations:
As a family destination, TCC gathers information on minors and children traveling with their parents/guardians. As a result, it is required to abide by COPPA (Children's Online Privacy Protection Act of 1998) regulations relevant to the collection of information on children under the age of 13. The act demands the enforcement of website privacy policies, requires consent from

parents or guardians for the collection of information on minors, and requires data collectors to "Maintain the confidentiality, security, and integrity of information they collect from children, including by taking reasonable steps to release such information only to parties capable of maintaining its confidentiality and security." A court can hold operators who violate COPPA rules liable for civil penalties of up to $46,517 per violation. As a result, TCC's client data requires rigorous oversight and a comprehensive security infrastructure due to the presence of this sensitive information as part of guest families.

International Regulations:
As a hotel that serves international guests, TCC may be subject to the EU's GDPR (General Data Protection Regulation) regulations if the hotel operates a website or other online service that is accessible to people in the EU. The regulation gives EU citizens the right to know what data is being collected about them, the right to request that their data be corrected or deleted, and the right to request that their data be transferred to another controller. Hotels are also required to appoint a data protection officer (DPO) and to implement appropriate technical and organizational measures to ensure the data's security. Failure to comply with GDPR can result in fines of up to €20 million or 4% of the company's global annual revenue, whichever is higher.

PCI-DSS (Payment Card Industry Data Security Standard) is a set of security standards established by major credit card companies, such as Visa, Mastercard, American Express, and Discover, to protect against credit card fraud and to ensure the safe handling and storage of sensitive cardholder information. The standard applies to TCC since it accepts credit card payments, regardless of the size or number of transactions. PCI-DSS compliance is mandatory and failure to comply can result in fines, penalties, or even the revocation of the ability to accept credit card payments.

Shifting Views of Consumer Safety

Inspired by the passing of the GDPR in Europe, American lawmakers in the state of California moved to pass the CCPA (California Consumer Privacy Act) in 2018, a law that gives California residents certain rights over their personal data. The law also requires that companies disclose if they are collecting personal information, and what categories of personal information they are collecting.

The CCPA has had a significant impact on the state of California, as well as other states in the US. It has prompted other states to consider passing similar legislation to protect their residents' personal data. Following California's lead, the states of Colorado, Connecticut, Utah, and Virginia will begin enforcing new GDPR-inspired statutes in 2023. The implications of this shift in the framework regarding data privacy protection will be profound in the years and decades to come and is likely to have major effects on how businesses are expected to secure consumer information, as well as expectations of greater transparency and accountability on the part of firms- particularly in the hospitality industry within which TCC operates. Although the state of

Nevada is yet to pass any specific legislation in response to these changes, it would be prudent for TCC to look into anticipating these incoming legal disruptions to the market environment to gain an edge over its competitors.

Some of the newly recognized rights that consumers and lawmakers are increasingly expecting from firms include the following:

- Access — The right to request access to inspect personal information.
- Correction — The right to request that errors in personal information be corrected.
- Portability — The right to request that personal information be transferred to another entity.
- Erasure — The right to request that personal information be deleted.
- Consent — The right to decide whether personal information may be sold or whether it may be used for purposes of receiving targeted advertising.
- Appeal — The right to appeal a business's denial of their request.

TCC would do well to keep these new expectations in mind when moving forward with their cybersecurity operations, as they underline an expectation for additional security when it comes to consumer information as well as more efficient and dynamic documentation and transfer of information between firms and consumers, meaning that existing legacy systems and storage organization methods may soon become obsolete.

Trust and Safety

According to the 2020 Trustwave Global Security Report, the hospitality industry ranked third among industries compromised by cybersecurity breaches in 2019 and suffered 13% of all attacks, two-thirds of which were attacks on corporate servers. Breaches like these can result in huge financial losses, operational disruption, and reputational harm, as well as expensive and time-consuming regulatory investigations and litigation.

Risks:

Penalties and Lawsuits:
Failure to properly secure client information and ensure transparency on the type of information collected as well as timely access to it when requested by clients could place TCC under legal repercussions, ranging from fines by local and international regulatory authorities to lawsuits by clients and staff members for breaches of information laws. Outside of lengthy and protracted legal proceedings, such penalties could also lead to a loss of trust from consumers, and the establishment of a negative reputation for TCC as an unsafe and poorly regulated firm.

Operational Disruption:
Hotels are already lucrative targets for hackers and other malicious actors due to their possession of lucrative client data on their HMS systems. Subpar protection against digital threats may be sufficient in other industries, but TCC faces the pressure of being a designated target of cyber attacks and can expect such incidents to harm its operational capacity if not addressed correctly. For example, attackers could take down the system in a DDOS attack. Such incidents would greatly disrupt the day-to-day business activity of TCC, in addition to creating an unsafe environment for guests and staff members.

Targeting and Harassment:
Attackers could use partial access to client information from TCC's HMS to carry out ransomware attacks targeting guests (a majority of attacks carried out against hospitality businesses in 2019 were ransomware attacks according to Trustwave), TCC staff, and other visitors. Such incidents would greatly disrupt the day-to-day business activity of TCC in addition to creating an unsafe environment for guests and staff members alike.

The value of T&S precautions:
Due to the factors mentioned above, we hope TCC's leadership can see the inherent value of investing in Trust and Safety precautions for the sake of clients, staff members, and TCC's integrity and transparency. Due to a rapidly changing legal environment, with new information safety regulations entering into effect across the United States, gaining an early advantage through a serious commitment to client privacy could save TCC the costs of being late to adapt to these new regulations. Additionally, as the threat of cyber attacks and privacy breaches takes up more public attention, providing a secure and private experience in the hospitality industry could become a unique selling point for TCC, having demonstrated its commitment to client security through a robust team of IT professionals. In this way, TCC would be able to instill consumer confidence and brand loyalty by positioning itself as a pioneering and forward-looking firm invested in the safety of its consumers.

Strategic Recommendations

Overall, TCC showed that they are really serious about their security with many earlier vulnerabilities getting patched and plenty of our recommendations getting implemented.

One of the things that had a great effect on TCC's infrastructure was network segmentation. It deterred many of our attack methodologies till TCC decided to provide us with more "white-box" access to their network. A real adversary would have a tougher time dealing with TCC's defenses. This makes our engagement representative of TCC's resilience against a worst-case scenario.

Overall, we recommend the following:

- Immediate patching of TCC's Domain Controller which is currently susceptible to a major exploit allowing remote code execution.
- Enforce stricter password policy, see details in technical findings.
- Enforce stricter account lockout and login policies to prevent brute-force and password-spraying attacks.
- Use Microsoft Edge + integrated kiosk mode on Guest Kiosks
- Implement logical rules to segregate guest and corporate networks.

Our recommendations correlate with NIST's guidelines which include a zero-trust architecture to mitigate cybersecurity risk, implementation of role-based access control, privileged access management, network segmentation, moving
target defense, and data protection. All applicable to TCC.

Engagement overview

Methodology

[redacted] testing methodology closely followed the official Penetration Testing Execution Standards (PTES) of seven stages: Pre-Engagement Interactions, Intelligence Gathering, Threat Modeling, Vulnerability Analysis, Exploitation, Post-Exploitation, and Reporting.

Pre-Engagement Interactions: The purpose of this section of the PTES is to show and explain the tools and techniques that are available to aid in the successful pre-engagement portion of a penetration test. The knowledge in this area is the result of many years of combined experience from some of the world's most effective penetration testers.

Intelligence Gathering: The objective of this section is to create a standard that is specifically developed for the pentester undertaking reconnaissance against a target (typically corporate, military, or related). When utilized correctly, it describes the thought process and aims of pen-testing reconnaissance and assists the reader in crafting a highly strategic plan for assaulting a target.

Threat Modeling: This section defines a threat modeling technique that is essential for proper penetration testing execution. The standard does not specify a model but rather demands that the model be consistent in its portrayal of threats, their capabilities, their qualifications as per the organization being evaluated, and their capacity to be applied to future tests with the same findings.

Vulnerability Analysis: Vulnerability analysis is the practice of identifying weaknesses in systems and applications that an attacker could exploit. These issues might range from misconfigured hosts and services to unsecured application architecture.

Exploitation: The exploitation phase of a penetration test is only concerned with gaining access to a system or resource by circumventing security limitations. If the vulnerability analysis in the previous phase was done correctly, this phase should be well-planned and have a precision strike. The primary goal is to identify the primary entry point into the business as well as high-value target assets.

Post-Exploitation: The goal of the Post-Exploitation phase is to identify the worth of the compromised machine and to keep control of the equipment for later usage. The sensitivity of the data stored on the machine and the machine's utility in further compromising the network determine the machine's worth. The methods described in this phase are intended to assist the tester in identifying and documenting sensitive data, identifying configuration

settings, communication channels, and relationships with other network devices that can be used to gain additional network access, and setting up one or more methods of accessing the machine at a later time.

Reporting: This section is meant to define the fundamental criteria for reporting upon penetration testing.

Scope

- 10.0.0.0/24 → corporate network
- 10.0.200.0/24 → guest network

Limitation

Given the limited scope of the penetration test, it should be emphasized that the resultant report and risk assessment are not exhaustive and that executing the recommended mitigations will not make The Cozy Croissant's network immune to all current and future dangers and cyber threats. The advice presented throughout this paper, on the other hand, will help to reduce already recognized vulnerabilities and, as a result, harden the entire network as a whole, decreasing not only current risks but also future threats.

Risk classification

Common Vulnerability Scoring System Measurement:
We used the Common Vulnerability Scoring System v3.1 (CVSS v3.1) to evaluate vulnerabilities on a technical level. CVSS is a widely acknowledged and open standard developed by the Computer Security Resource Center (CSRC) of the National Institute of Standards and Technology (NIST). CVSS assesses a vulnerability's complexity, accessibility, and influence on a system's confidentiality, integrity, and availability. We used the CVSS v3.1 calculator from the National Vulnerability Database (NVD) to calculate CVSS. The outcomes of the assessment are categorized into five levels of security risk: Critical, High, Medium, Low, or Informational. These classifications are based on industry best practices and may differ from internal risk perceptions. As such, we suggest that TCC reclassify these findings based on their tolerances for different business risks, with assistance from the business risk index.

Rating	CVSS Score
Informational	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

The following scale describes the general implications of each risk assessment rating:

Critical Risk: Presents an immediate and direct risk to the client; likely to have major implications on the legal, financial, or reputational state of the firm; considered a violation of industry regulations.

High Risk: Presents a serious risk to the operations of the system which may render it highly unusable, unsafe, or inefficient to users if exploited and/or unremedied.

Medium Risk: Presents a moderate risk to the operation of the system and the experience of users if exploited and/or unremedied.

Low risk: Presents a minor risk to the operation of the system and the experience of users if exploited and/or unremedied.

Informational: Virtually no risk to clients or system operations, reported as part of due diligence as encountered during the penetration test.

Business Impact Measurement:

While the CVSS parameters provide guidelines for technical shortfalls in the system, many of these will naturally have real-world business implications that affect TCC's finances, management, accounting, or marketing and image. As such, a rudimentary business impact matrix was used to place these more subjective risks into perspective and assist with the prioritization of different system vulnerabilities.

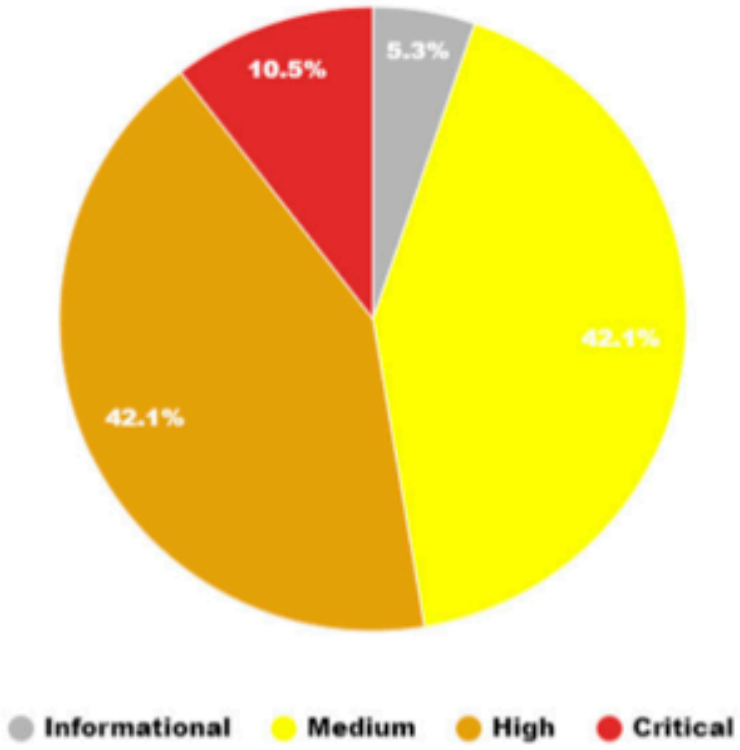
Likelihood \ Impact	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low Med	Medium	Med Hi	High	High
Likely	Low	Low Med	Medium	Med Hi	High
Possible	Low	Low Med	Medium	Med Hi	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	Med Hi
Very Unlikely	Low	Low	Low Med	Medium	Medium

Technical Findings

The following scale is used to show the priority of vulnerabilities based on the CVSS scores which was calculated using the NVD CVSS v.3.1.

Informational	Low	Medium	High	Critical
1	0	8	8	2

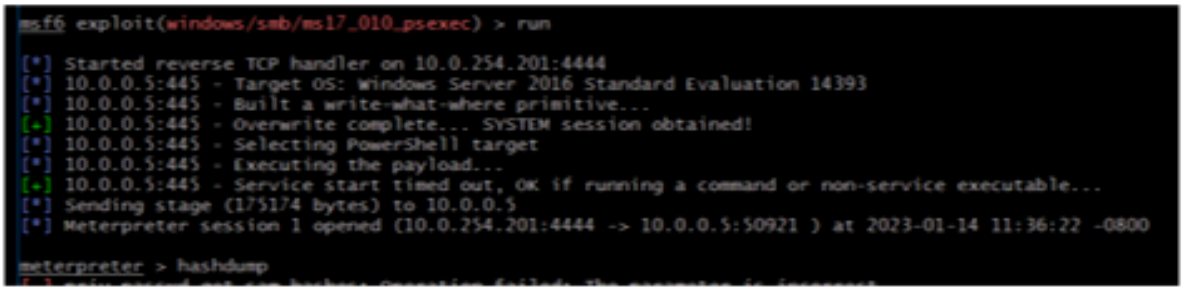
Also attached is the graphical representation of the number of vulnerabilities found.



CVSS: 9.5	Domain controller vulnerable to MS17-010 EternalBlue
	10.0.0.5

Description: The TCC Domain Controller was vulnerable to the notorious MS17-010 EternalBlue vulnerability. A serious vulnerability that affects Microsoft Windows' SMBv1.
Impact: A completely unauthenticated malicious actor can achieve remote code execution on TCC's domain controller, handing them control over all of TCC's computers, users and client data.
Remediation: Apply latest Windows updates.
Replication:

- Inside Metasploit, run the windows/smb/ms17_010_psexec module with RHOST set to 10.0.0.5



References:

- https://www.hypr.com/security-encyclopedia/eternalblue

CVSS: 9.0	Weak Passwords / Unenforced Password Policy
	10.0.0.0/24

Description: Passwords across TCC's COZY domain are cryptographically weak and hence easy to crack.
Impact: A malicious actor that is able to obtain password hashes can crack them in a matter of minutes with limited computational resources.
Remediation: Enforce a good password policy, see reference.
Replication:

- Running hashcat with a mode 1000 and the standard "rockyou" wordlist.
    - hashcat -m 1000 tcc_hashes.txt /usr/share/wordlist/rockyou.txt

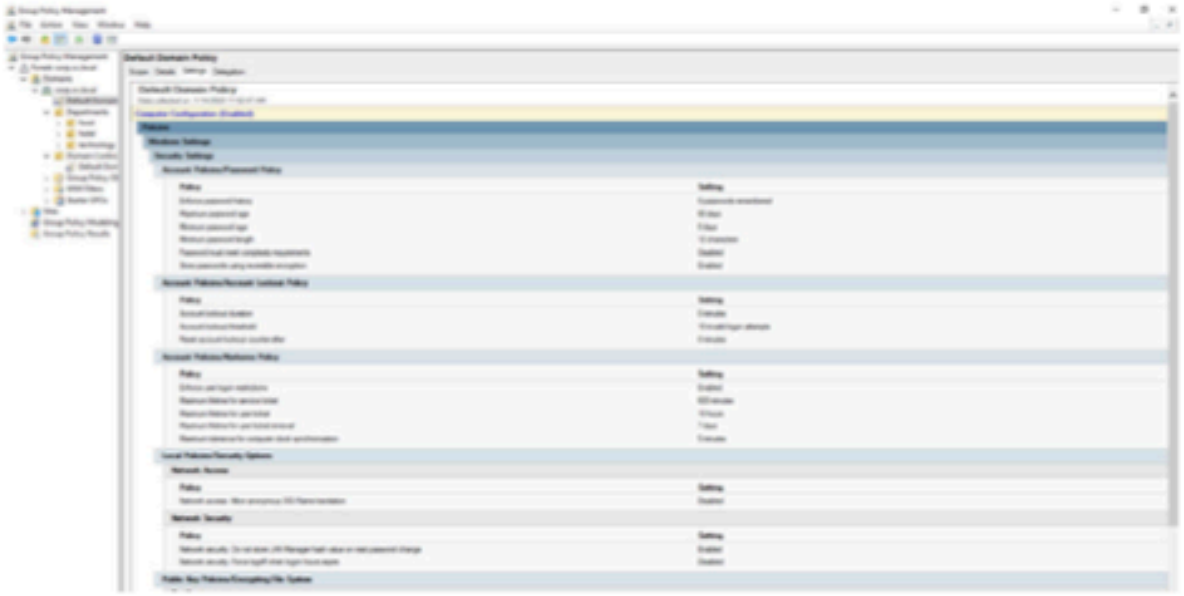
References:

- https://learn.microsoft.com/en-us/microsoft-365/admin/misc/password-policy-recommendations?view=o365-worldwide

CVSS: 6.4	Weak account policy configuration
	10.0.0.0/24

Description: Weak lockout and login policies are present on TCC's corporate network.
Impact: Enables brute-force and password-spraying attacks which can result in critical user account compromise on TCC's corporate network.
Remediation: Use sensible lockout and login policies. See Microsoft guidelines in references.
Replication:

- In the domain controller, open Group Policy Management and view Default Domain Policy



References:

- https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/account-lockout-policy

CVSS: 8.5	Outdated Wordpress version
	10.0.0.11

Description: An outdated WordPress version (4.8) is used as TCC's Hotel Management System.

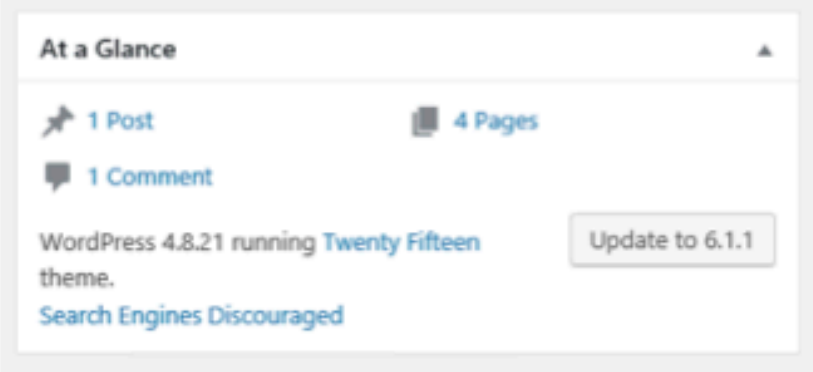
Impact: Outdated software is a primary cause of compromise in enterprise networks as they are prone to popular, publicly available exploits.

Remediation:

- Update WordPress to latest version.

Replication:

- Wordpress dashboard (At a Glance) shows the installed WordPress version.



CVSS: 7.1	Wordpress Lack of Role-Based Access Control
	10.0.0.6

Description: TCC's Hotel Management System includes a single admin user for all management tasks.

Impact: The lack of different, separate user accounts representing different duties provides a single-point-of-failure where TCC's entire management system gets compromised once the admin user is compromised. It also makes management difficult as TCC operations scale and more employees manage TCC's HMS.

Remediation:

- Create different admin accounts
- Assign different roles to these admins accounts. Example: A dedicated admin account for making reservations, another for changing website settings, another for reviewing financial data, etc. Wordpress' and SOLIDRES' (TCC's hotel management/reservation plugin) tabular design allow for intuitive and easy implementation of access control.

Replication:

- Checking the User tab on Wordpress showed a single admin user account, with full privileges.

CVSS: 6.3	Wordpress Insecure Login Confirmation Messages
	10.0.0.6

Description: The Wordpress deployment (used for TCC's Hotel Management System) discloses sensitive information on the admin login form.

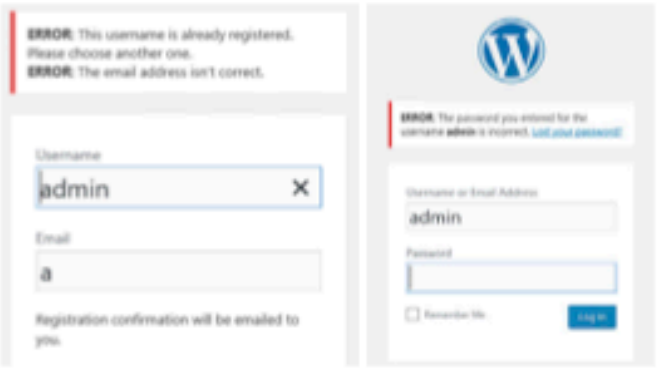
Impact: This common vulnerability allows a malicious actor to enumerate admin usernames, significantly reducing the number of attempts required for a successful bruteforce attack.

Remediation:

- Update Wordpress version as newer versions should not have this vulnerability, although we were unable to check. See next point.
- Use a custom Wordpress login plugin such as wp-login-form to create a secure, custom alternative. See references.

Replication:

- On /wp-admin, visit the Register New Account page. The associated form confirmation allows for username enumeration.
- On the same page, the Login form also allows for username confirmation.



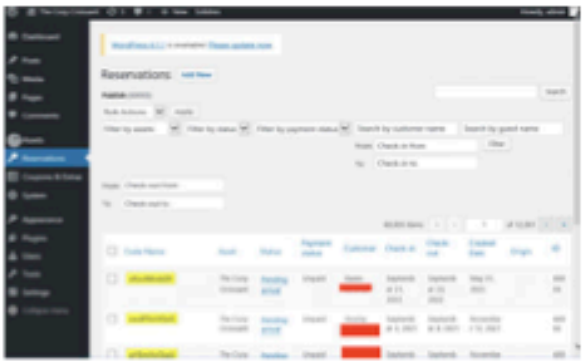
References:

- https://wordpress.org/plugins/wp-login-form/

CVSS: 9.1	Wordpress Default Credentials
	10.0.0.11

Description: The hotel management system running on 10.0.0.11 has default Wordpress credentials. Whilst it is understandable that this is sensible given the fact that the TCC's HMS is only internally facing, TCC should still adopt a multi-layered approach to security. Such an approach would render TCC resilient even in the unlikely event of malicious public access to the hotel management system.

Impact: An attacker with low-privilege access to the host 10.0.0.11 can view all reservation information and PII information of TCC's clients.



Remediation: Strong passwords must be used even on purely internally faced services. Especially when they are as business critical as TCC's HMS.

Replication:

- After gaining access through RDP to host 10.0.0.11, navigate to http://localhost/admin
- Log in using username: admin, password: password

CVSS: 5.1	Kiosk File Inclusion
	10.0.200.[101,102,103,104]

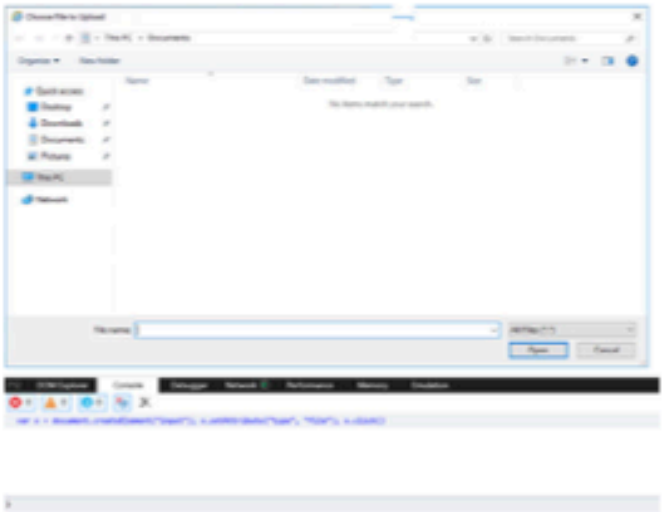
Description: Using the developer console, a user can launch a Windows Explorer tab. With this tab, a malicious actor can navigate within the local file system, and discover what lies on it, and read and modify content.

Impact: A malicious actor can gain access to read or modify any files on the local file system. Further exploits including RCE are also enabled through this.

Remediation: Upgrading to Microsoft Edge and utilizing the built-in kiosk mode (see references) allows for an automatic and well-tested method for configuring a sandboxed kiosk browser. By utilizing Edge, a well supported program, TCC is less likely to be susceptible to simple attack vectors and misconfigurations.

Replication:

1. Starting from the regular kiosk start page, right click and select "Inspect Element"
2. In the developer tools menu, select the console, and run the following snippet:
   var x = document.createElement("input"); x.setAttribute("type", "file"); x.click()
3. A file explorer window should now be open.
4. Replace iexplorer.exe binary with cmd.exe binary.
5. Obtain shell access on TCC's Guest kiosk.



References:

Microsoft Edge Kiosk Mode:
https://learn.microsoft.com/en-us/deployedge/microsoft-edge-configure-kiosk-mode

CVSS: 5.1	Kiosk Elevated Account Permissions
	10.0.200.[101,102,103,104]

Description: The kiosk machines have the default Administrator account enabled with no password. This allows any user access to an admin account, which opens up further exploits.

Impact: A malicious actor is able to execute any operation in Administrator mode, bypassing most protections put in place by windows. This includes accessing and modifying security properties, running scripts with full permissions, and modifying critical system components.

Remediation: Create low-privilege user accounts for each guest automatically, either utilizing room number of other guest information to allow logging in. These accounts should only have the minimum required permissions for the desired functionality.

CVSS: 6.3	Kiosk Arbitrary Code Execution
	10.0.200.[101,102,103,104]

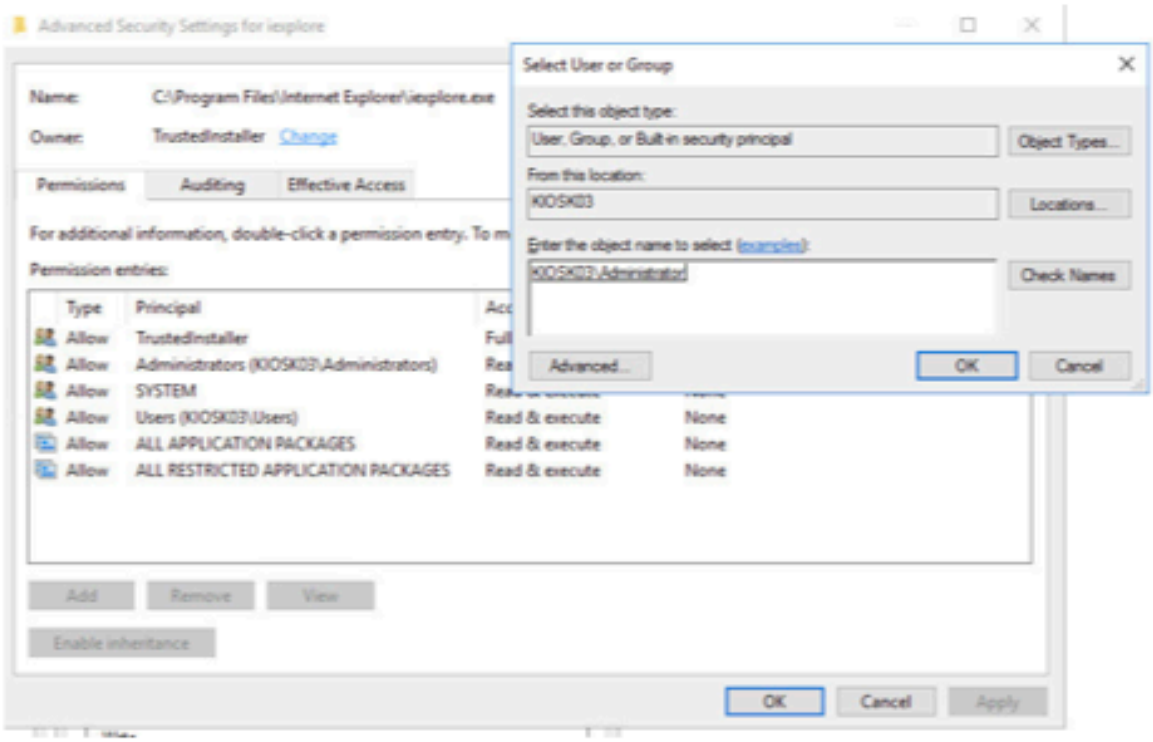
Description: Using the file inclusion and the unprotected administrator account, a user can right click on any file and run. If used with a shortcut to CMD, it's possible to execute arbitrary commands.

Impact: A malicious actor is able to execute any commands they desire on the system, giving them near limitless control over the kiosk system. They can modify files, change settings, disable features, and gain complete power over the operation of the system.

Remediation: Do not use an account which has write and run permissions on the kiosk, to prevent the running of the commands.

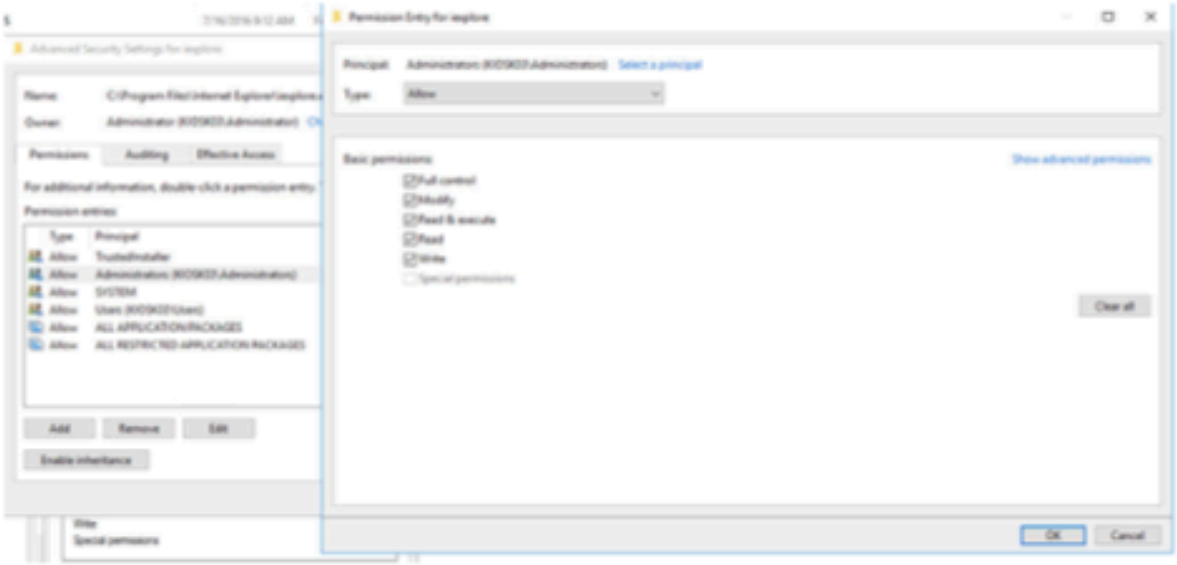
Replication:

1. Follow the steps from "Kiosk File Inclusion" to gain an explorer window.
2. Navigate to C:\Program Files\Internet Explorer
3. Right click on iexplore.exe and select Properties
4. In IE properties, select Security -> Advanced -> Click "Change" under "Owner". Type Administrator in the window that loads and click "Check Names"

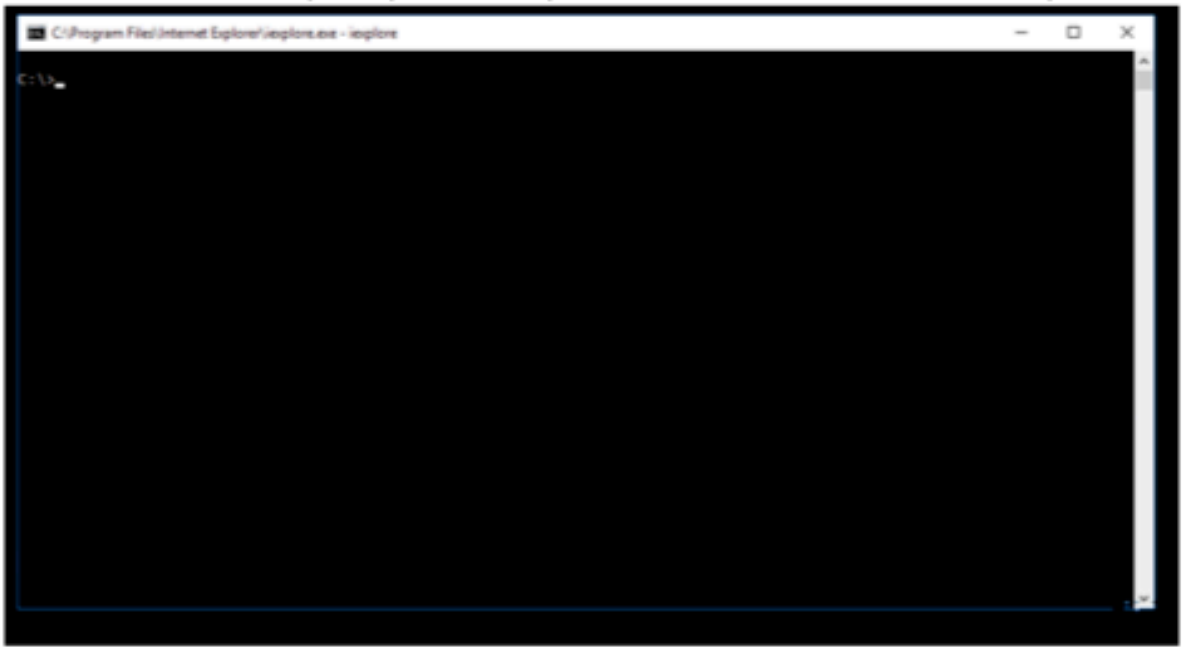


5. Click Ok -> Apply, then close the properties window.

6. Reopen the properties window and click on Change Permissions -> Administrators (Kiosk03\Administrators) -> Enable Full Control. Apply and close out of the menu



7. Rename iexplore.exe to anything else
8. Copy the binary for cmd.exe from C:\Windows\System32\cmd.exe to the Internet Explorer folder, and rename it to iexplore.exe
9. Close out of the file upload menu, and click ctrl+f4. This will exit internet explorer, which will be restarted by the system. The system will now launch the new cmd binary.



CVSS: 7.7	Kiosk SMB Servers
	10.0.200.[101,102,103,104]

Description: The guest kiosks are running SMB servers, which combined with the unprotected Administrator account allow malicious actors access to read the server files, or copy files onto the server.

Impact: A malicious actor can enumerate all the files on the server and download them. They can upload custom and malicious software to be run.

Remediation: The kiosk servers should not have public SMB servers running, and the administrator account should not be activated and unlocked during normal operation.

Replication:

- Any SMB client is able to connect to the server, for instance using smbclient:
    - smbclient -U Administrator kiosk01.guest.cc.local

CVSS: 8.6	Kiosk DOS Attack
	10.0.200.[101,102,103,104]

Description: By utilizing the same methodology as the “Kiosk Arbitrary Code Execution” exploit, the server can be configured to run a corrupt/invalid binary, which would cause the server to continuously crash on program startup. This exact denial of service was performed by our team to Kiosk 1 as communicated in a support ticket.

Impact: A malicious actor is able to completely disrupt the activity of the kiosk, and prevent guests from interacting with it. It is also possible to configure the kiosk to display inappropriate or undesired content on the screen.

Remediation: This specific exploit doesn’t have any specific exploits, however the remediation techniques mentioned in related issues (such as "Kiosk File Inclusion") resolve the issue.

Replication:

1. Follow the steps of “Kiosk Arbitrary Code Execution” up to step 8.
2. Copy a malicious or corrupt executable into the Internet explorer folder and rename it to “iexplore.exe”.
3. Restart the internet explorer tab, and the new binary will be launched.

CVSS: 7.3	Media Server Unauthenticated Administrator Privileges
	10.0.0.20

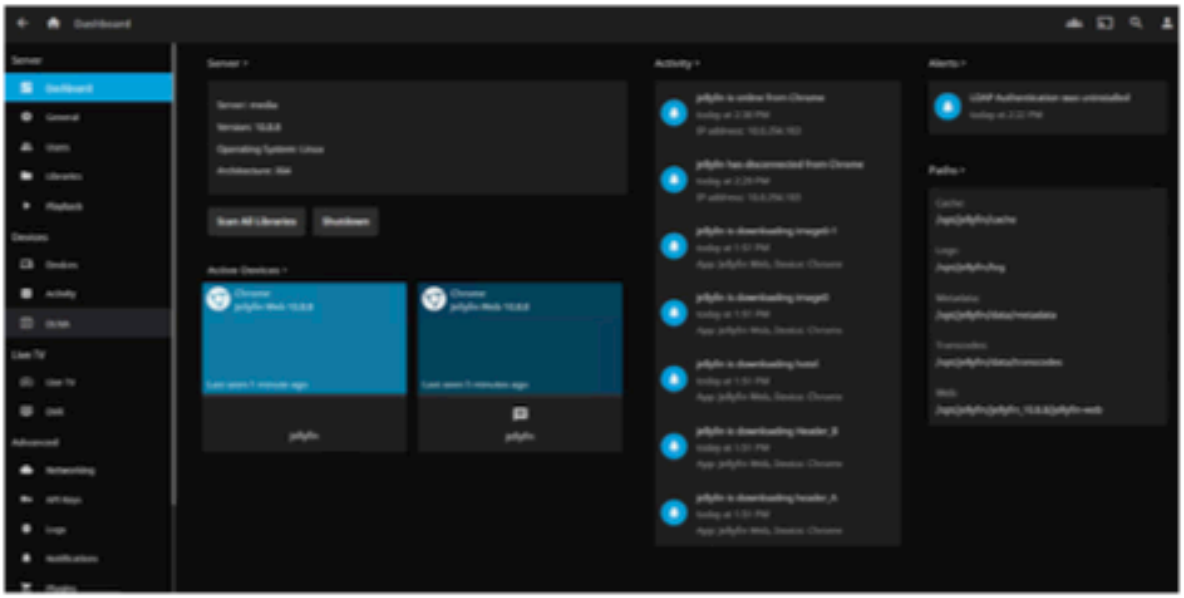
Description: Any user can access the administrator account on the Jellyfin application.

Impact: A malicious actor can upload media to the server without any authentication. In addition, they can view folders on the web server.

Remediation: Protect the administrator account using a strong password

Replication:

- Visit 10.0.0.20 on 80/tcp



CVSS: Informational	Guest/Corporate Network Isolation
	10.0.0.0/24, 10.0.200.0/24

Description: The guest and corporate networks are open to each other, despite neither relying on the other. This allows malicious actors to transition from one compromised host to other hidden internal hosts.

Impact: A malicious actor can attack the corporate network as though they were acting from an internal network or host. This might allow them to skip some firewalls or access control systems.

Remediation:

- Implement logical rules preventing communication between TCC's Guest (10.0.200.0/24) and Corporate (10.0.0.0/24) networks. This can be done using a simple host-based firewall.

Replication:

- Boxes on the corporate network are accessible by Guest kiosks.

CVSS: 8.7	Plain-Text Credentials in API token
	10.0.0.12

Description: The rewards system API running on (10.0.0.12) stores credentials in plain-text.
Impact: Guests that reuse passwords will be at a much higher risk of having other accounts compromised by an adversary.
Remediation: All passwords must be hashed before entering the database. Furthermore, the hash must not be sent to the front end of the web application and instead be validated in the back end.
Replication:

CVSS: 5.6	Credential-Exposing API
	10.0.0.12

Description: The rewards system API sends back all the user information (including password in plain-text) back to the user regardless of the validity of the provided password.
Impact: An attacker can gain access to the rewards account and personal information of any guest using only their username.
Remediation: Authentication should happen only on the backend without exposing any account information.
Replication:

- Make a request to the login API using curl
    - curl "https://10.0.0.12/userapi.php?login&;type=user;user=<username>;pass=<password>"
    - Replace <username> with a valid username, and <password> with any text
- The API responds with the correct credentials of the user

CVSS: 6.4	Misconfigured User Privileges
	10.0.0.12

Description: All users on the reward system have administrator privileges and can dump all the credentials of other users.
Impact: A malicious actor is able to gain access to the private information of hundreds of guests including usernames, emails, and plain-text passwords
Remediation: Normal users must be given the least possible privileges
Replication:

- The core.js file contains a function for querying all users which requires the secret token of any administrator account.
- The secret token can be obtained by capturing the json response by authenticating to the API.

CVSS: 7.8	Fixed Output from Password Generator
	10.0.0.51, 10.0.0.52

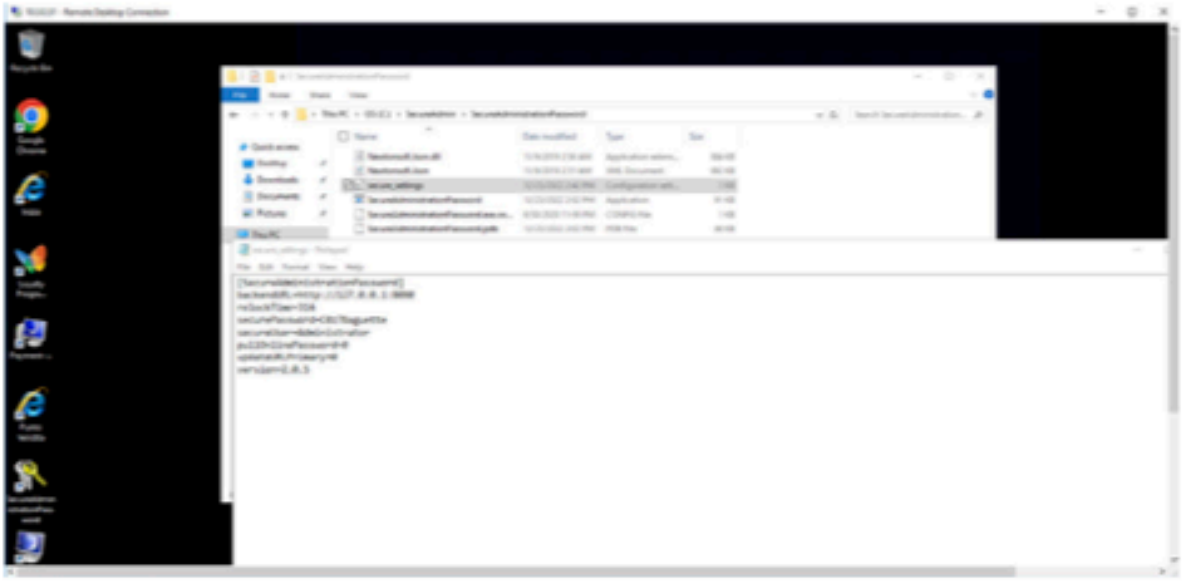
Description: An application of the name "SecureAdministratorPassword" was present on TCC's workstations. The application seems to serve the purpose of generating secure passwords to be used by TCC employees; however, looking at the application's configuration files, it was shown that it generates the same passwords.

Impact: An unsuspecting user might use the application to generate a "secure" password which will accidentally lead to password reuse and potential account compromise.

Remediation: Uninstall SecureAdministratorPassword from TCC's environment.

Replication:

- Navigate to OS\SecureAdmin\SecureAdministratorPassword\secure_settings.conf



CVSS: 4.3	Exposed Default IIS Server Deployment
	10.0.0.6

Description: A fresh, default deployment of Microsoft IIS server is publicly exposed.

Impact: Unattended default deployments often suffer from misconfigurations and are prone to future zero-days. In all instances, TCC should be aware of this running IIS instance and/or terminate it if it serves no purpose.

Remediation: Terminate redundant Microsoft IIS server.

Replication: Visit http://10.0.0.6 or http://adcs.corp.cc.local