Vulnerability Assessment

December 8th, 2024

Brick Wall Cyber

Security Assessment Team

Mamadu Bah	Principal Analyst
Susan Olayemi	Security Analyst
Aemon Moyer	Security Analyst
Zach Lukas	Security Analyst

Division of Responsibilities

Student	Expected Contributions
Susan	4 Vulnerabilities, Section 2: threat and Risk
Mamadu	4 Vulnerabilities, Section 3: Summary of Results
Zack	4 Vulnerabilities, executive summary
Aemon	4 Vulnerabilities
Communication Plan	
Communication through Discord	
Meeting Schedule	
N/A	

1. EXECUTIVE SUMMARY

Our security assessment team was tasked with completing a security review of Brick Wall Cyber's network ecosystem. The review was performed during the time frame of October 29, 2024, to December 9, 2024. This report provides a high-level overview of vulnerabilities discovered, their relevance and potential impact on Brick Wall Cyber's continued operation, and which vulnerabilities are of most immediate concern.

Project Objectives:

To find what vulnerabilities are present in Brick Wall Cyber's infrastructure a threat actor could exploit in order to infiltrate said infrastructure.

Overview of Findings:

The majority of vulnerabilities found ranged from Medium risk to Critical risk (3 critical, 8 high, 5 medium CVSS ratings), with 10 out of 16 vulnerabilities found having a prioritization of immediate or short. Put simply, Brick Wall Cyber's infrastructure has many dangerous vulnerabilities that need to be addressed as soon as possible.

Summary of Findings:

The most egregious findings fall into 3 categories:

Confidentiality of Data: these vulnerabilities allow for leaking of confidential data
Privilege Escalation and Remote Execution Vulnerabilities: these vulnerabilities allow for an attacker to remotely access Brick Wall Cyber systems, run malware, or even take complete control of a system.
Potential Exploitation Within Critical Infrastructure: these vulnerabilities allow attackers to change account permissions or disable security controls.

Summary of Recommendations:

- Regularly update systems and enable automatic updates.
- Implement strong access management systems, such as Multi-Factor Authentication, and put into practice a policy of least privilege.

- Invest In Security Awareness Training for Staff.

2. THREATS AND RISK

2.a Threat Assessment

2.a.1 Threat Actor Motivations

Motivation	Relevance to Brick Wall Cyber
Money	Given that BWC is a cybersecurity firm that holds sensitive information about its clients. The threat actor could perform ransomware attacks, knowing that BWC will likely pay it to protect its reputation and prevent its clients' sensitive information from being leaked.
Ideology	Provided that BWC has top corporations or the government as clients, The threat actor in a form of protest would likely attack BWC to oppose the cooperations or the
Coercion	Similarly to the motivation of money, the threat actor could pressure BWC into refusing clients that are against the threat actor through ransomware, or DDoS attack.
Ego	Given that BWC is a cybersecurity firm that holds sensitive information about its clients. The threat actor could attack BWC for glory and reputation.

Motivation	Relevance to Brick Wall Cyber
Reciprocation	The attacker could use existing relationships with clients, staff, or partners to gain unauthorized access to sensitive information and internal systems causing a significant breach and threat to BWC.
Authority	The attacker could impersonate a person of authority, in order to trick the staff into revealing

	sensitive information leading to data leaks, loss of reputation, and loss of clients.
Scarcity	The attacker could manipulate BWC clients, staff, or partners into releasing sensitive information by alerting limited availability of things, manipulating them into giving access, or releasing sensitive pieces of information. The limited availability could include urgent fixes and updates and limited-time discounts on cybersecurity products and services.
Commitment / Consistency	The attacker using commitment/consistency could manipulate employees, clients, or partners into providing unauthorized access, exposing sensitive information, or allowing security breaches. Which could pose significant damage to BWC
Liking	The attacker could pose as a new client who wants to know more about services while building a very good rapport with the staff. Then slowly influence making it easier to manipulate them to release sensitive information and grant access to critical systems.
Social Proof	The attacker could manipulate BWC clients, staff, or partners by impersonating a colleague or trusted higher-positioned staff and acknowledging that exposing sensitive information or any type of confidential situation in the company helped gain promotions or money. Ultimately, this will have a very high significance on BWC.

2.a.2 Threat Model

Threat	High-level Mitigation	Importance for Brick Wall Cyber (Low/Medium/High)
Spoofing	Short	Low
Tampering	Long	Medium
Repudiation	Long	Medium
Information Disclosure	Imme.	High
Denial of Service	Imme.	High
Elevation of Privilege	Imme.	High

2.b Risk Matrix

RISK MATRIX		THREAT IMPACT			
		LOW	MEDIUM	HIGH	CRITICAL
LIKELIHOOD	RARE	Low	Low	Medium	Medium
	UNLIKELY	Low	Medium	High	High
	LIKELY	Low	Medium	High	Critical
	VERY LIKELY	Low	Medium	Critical	Critical

2.c Prioritization Categories

Mitigation Priority	Description
Immediate (Imme.)	The finding has a critical business impact, likelihood, and risk. It damages the operation of the client. Finding causes a direct violation of regulation, law, or compliance that applies to the client. Finding leaks of Personally Identifiable Information, Sensitive Information, or information that can lead to further access to sensitive data. The finding is related to previous indicators of compromise and suggests the occurrence of past cyberattacks.
Short-term (Short.)	Finding has a high business impact, likelihood, and risk. It partially damages the operation of the client and has the potential for further exploitation. Finding gives attackers direct access to a system or a service. Finding allows the attackers to violate Confidentiality, Integrity, Availability of a system.
Long-term (Long.)	Finding has a medium business impact, likelihood, and risk. Finding is related to security misconfigurations which can lead to further potential attacks. Finding allows attackers to partially violate Confidentiality, Integrity, Availability of a system.
Eventual (Evetl.)	Finding has a low business impact, likelihood, and risk. Finding is not following the best security practices. Finding is a bug or an unintentional mistake that has little to no security implication.

3. SUMMARY OF RESULTS

3.a Key Findings

3.a.1 Vulnerabilities Impacting Confidentiality of Data

Vulnerabilities such as CVE-2024-8775 allow any data stored within an Ansible Vault to be leaked in plaintext through poor security practices such as mishandling encryption and a lack of secure programming. This vulnerability occurs when the playbook, a list of commands, is executed and the data is shown by printing the playbook output. Given the nature of the vulnerability, it is possible that this vulnerability could lead to attackers exploiting this vulnerability to expose data leaks, or potentially lead to users unintentionally

3.a.2 Numerous Privilege Escalation and Remote Execution Vulnerabilities

Threats such as CVE-2019-1484 pose a great risk to the infrastructure of BrickWall Cyber as they lead to a malicious remote code execution through mishandling Windows Object Linking and Embedding (OLE), leading to malicious files being misrepresented as regular files. When this remote is executed, attackers can get remote access and run malware on the compromised host. Privilege escalation vulnerabilities such as CVE-2020-1467 allow attackers to control an affected system through Windows hard links.

3.a.3 Potential Exploitation Within Critical Infrastructure

Active Directory and AlienVault OSSIM are two pieces of critical infrastructure. Active Directory is a tool used for operations such as user and account management. AlienVault OSSIM is a security platform that collects event data and performs security assessments in order to protect a network. However, within Brick Wall Cyber there are multiple opportunities for exploitation. For example, CVE-2021-42291 allows users to change security-related configurations on objects stored within Active Directory. CVE-2016-8582 is a vulnerability on AlienVault OSSIM which allows attackers to to exploit an SQL query.

3.b. Key Recommendations

3.b.1 Establish a Proper Update Strategy

Some vulnerabilities mainly occur in older systems. Critical vulnerabilities such as CVE-2021-44228 deal with a malicious arbitrary code execution if the host contains any Apache Log4j2 for versions 2.0 until 2.15. BrickWall Cyber should continuously look out for any new security patches on any pieces of infrastructure to ensure protection against any potential exploits. It's also recommended to configure automatic updates which leaves out any potential opportunity for human error.

3.b.2 Implement Strong Access Management Systems

In order to avoid any potential privilege escalation, it's important that BrickWall Cyber implements strong access controls. Some recommended methods of implementing a stronger access management system is by setting up Multi-Factor Authentication to prevent any unauthorized users. It's important to also utilize the principle of least privilege which ensures that users of the application receive the adequate roles required for their role.

3.b.3 Invest In Security Awareness Training for Staff

Because BrickWall Cyber contains many systems, such as Active Directory, which holds access to many sensitive data, staff must understand how to handle this data. Investing in security training will allow staff to understand how to properly handle sensitive data and information within the company. Not only will the staff be able to handle this data, but training will also ensure that they can effectively respond to any threats to data or systems within BrickWall Cyber.

3.c. Response Plan

Mitigation Prioritization	Vulnerability

Immediate (Imme.)	• CVE-2019-1484 • CVE-2020-1467 • CVE-2016-8582 • CVE-2024-6387 • CVE-2021-42291 • CVE-2021-44228
Short-term (Long.)	• CVE-2024-5187 • CVE-2023-29975 • CVE-2019-9510 • CVE-2023-34367
Long-term (Short.)	• CVE-2011-3351 • CVE-2024-8775 • CVE-2024-46538 • CVE-2022-21132 • CVE-2024-0115
Eventual (Evetl.)	• CVE-2019-0581

4. VULNERABILITIES

4.a CVE-2019-1484

Risk Analysis		CVSS	Prioritization
Risk	**Critical**	**7.8 High**	**Imme.**
Impact	**CRITICAL**		
Likelihood	**VERY LIKELY**		
Hosts Impacted	File Server Windows 2k19		

Description
When Microsoft Windows Object Linking and Embedding, which allows Office applications to interact with other applications, fails to properly validate user input, a remote code execution gives an attacker the opportunity to open a specific file which leads to Windows executing arbitrary code. Since File Servers tend to store sensitive data, by exploiting this vulnerability, hackers can access critical files essential to the company

External References
https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2019-1484 https://nvd.nist.gov/vuln/detail/cve-2019-1484

4.b CVE-2020-1467

Risk Analysis		CVSS	Prioritization
Risk	**Critical**	**7.8 High**	**Imme.**
Impact	**Critical**		
Likelihood	**Highly Likely**		
Hosts Impacted	Windows 7, Windows 8, Windows 10		

Description
This vulnerability presents a potential elevation of privilege attack through the mishandling of Windows hard links. Hard links essentially allow the system to have more than one name for the same file. If exploited properly, an attacker can overwrite a file which could lead to an elected status in privileges. This is dangerous for BrickWall Cyber as an attacker can gave admin privileges on any Windows 7,8 or 10 machine.

External References
https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-1467 https://nvd.nist.gov/vuln/detail/cve-2020-1467

4.c CVE-2016-8582

Vulnerability Name		CVSS	Prioritization
Risk	**Critical**	**9.8** **Critical**	**Imme.**
Impact	**Critical**		
Likelihood	**Very Likely**		
Hosts Impacted	Alienvault ossim		

Description
AlienVault OSSIM (Open Source Security Information and Event Management) is used to collect security event data across a network. AlienVault, there is a vulnerability in gauge.php that allows attackers to execute an SQL query and retrieve information from databases. If BrickWall Cyber is not updated to 5.3.2 they could suffer potential database leaks since AlienVault is utilized within their infrastructure.

External References
https://www.incibe.es/en/incibe-cert/early-warning/vulnerabilities/cve-2016-8582 https://nvd.nist.gov/vuln/detail/CVE-2016-8582

4.d CVE-2011-3351

Risk Analysis	CVSS	Prioritization

Risk	**medium**	**7.1 High**	**Long.**
Impact	**medium**		
Likelihood	**unlikely**		
Hosts Impacted	OpenVAS		

Description
OpenVas scanners that are before 2011-09-11 will insecurely create a file while generating system configuration documents. This allows attackers to use this vulnerability to overwrite files on the system. If BrickWall Cyber does not have a current version of OpenVAS, any files within the system are subjected to potential overwriting from the attackers.

External References
https://nvd.nist.gov/vuln/detail/CVE-2011-3351 https://avd.aquasec.com/nvd/2011/cve-2011-3351/

4.e CVE-2024-6387

Vulnerability Name		**CVSS**	**Prioritization**
Risk	**High**	**8.1 high**	**Imme.**
Impact	**High**		
Likelihood	**likely**		
Hosts Impacted	Ssh jump		

Description
This vulnerability enables attackers to gain full root access to a system without any user interaction, making it extremely critical for jump servers. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period. This would likely impact Brick Walls Cyber because an unauthenticated user having root access to the server could impact the client's abilities to travel to the gateway to their desired destination in the BWC infrastructure. This could lead to lack of availability and possibly

integrity because the unauthenticated attacker could change the information in BWC systems causing confusion.

External References
https://nvd.nist.gov/vuln/detail/cve-2024-6387 https://www.mamori.io/blog/mitigating-jump-server-security-risks

4.f CVE-2021-42291

Risk Analysis		CVSS	Prioritization
Risk	**critical**	**8.8** **Critical**	**Imme.**
Impact	**critical**		
Likelihood	**likely**		
Hosts Impacted	Active Directory		

Description
Active Directory Domain Services Elevation of Privilege Vulnerability. A security bypass vulnerability that allows certain users to set arbitrary values on security-sensitive attributes of specific objects stored in Active Directory (AD). This would likely impact Brick Wall Cyber because if the attacker has access to the active Directory they get access to sensitive information through elevating their status/role. Allowing for leaks and breach in confidentiality that brick wall cyber offers.

External References
https://nvd.nist.gov/vuln/detail/CVE-2021-42291 https://www.riskinsight-wavestone.com/en/2023/06/surviving-an-active-directory-compromise-key-lessons-to-improve-the-reconstruction-process/

4.g CVE-2024-8775

Risk Analysis	CVSS	Prioritization

Risk	**medium**	**5.5 medium**	**Long.**
Impact	**medium**		
Likelihood	**likely**		
Hosts Impacted	Ansible		

Description
A flaw was found in Ansible, where sensitive information stored in Ansible Vault files can be exposed in plaintext during the execution of a playbook. This can lead to the unintentional disclosure of secrets like passwords or API keys, compromising security and potentially allowing unauthorized access or actions. This would likely impact brick wall cyber because this is an internal problem from Ansible, but it can still be prevented by setting the no_log: true parameter. This would need immediate and long term prioritization because sensitive information can be given unintentionally to unauthorized personnels causing data leaks.

External References
https://nvd.nist.gov/vuln/detail/CVE-2024-8775 https://www.ansible.com/

4.h CVE-2021-44228

Risk Analysis		**CVSS**	**Prioritization**
Risk	**critical**	**10.0 Critical**	**Imme.**
Impact	**critical**		
Likelihood	**Unlikely**		
Hosts Impacted	ELK		

Description

An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. BWC will unlikely be impacted by this because this vulnerability has been disabled from this host. This prevents this specific vulnerability from impacting BWC.

External References
https://www.elastic.co/security-labs/detecting-log4j2-with-elastic-security https://nvd.nist.gov/vuln/detail/CVE-2021-44228

4.i CVE-2024-5187

Risk Analysis		CVSS	Prioritization
Risk	**Medium**	**8.8** **High**	**Short.**
Impact	**High**		
Likelihood	**Rare**		
Hosts Impacted	Kali Linux		

Description
A vulnerability in the onnx framework that allows attackers to overwrite any file on the system. The impact is High because the ability to overwrite any file on the system is very dangerous ability for an attacker to have. The likelihood is low because we are not certain if Brick Wall Cyber even has the onnx framework. If BWC does use this framework however, then this would be a vulnerability of concern. Because this vulnerability depends on the presence of the onnx framework, which is not a very popular application for someone to have, only targeted attackers that know BWC uses this framework would exploit this vulnerability, thus the low likelihood.

External References
https://www.cve.org/CVERecord?id=CVE-2024-5187

4.j CVE-2023-29975

Risk Analysis	CVSS	Prioritization

Risk	High	7.2 High	Short.
Impact	High		
Likelihood	Likely		
Hosts Impacted	Pfsense 2.6.0		

Description
Allows attackers to change the password of any user, without needing authentication. For Brick Wall Cyber, this means that not only could an attacker prevent employees from logging in, but the attacker could also log in as that employee with the new password.

External References
https://www.cve.org/CVERecord?id=CVE-2023-29975 https://nvd.nist.gov/vuln/detail/CVE-2023-29975

4.k CVE-2024-46538

Risk Analysis		CVSS	Prioritization
Risk	Medium	4.8 Medium	Long.
Impact	Medium		
Likelihood	Likely		
Hosts Impacted	Pfsense 2.5.2		

Description
A cross-site scripting vulnerability that allows arbitrary execution of HTML or web scripts. For Brick Wall Cyber, this could be the start of a larger attack. An attacker could use web scripts to launch a larger attack with a more dangerous exploit.

External References

https://www.cve.org/CVERecord?id=CVE-2024-46538 https://nvd.nist.gov/vuln/detail/CVE-2024-46538

4.l CVE-2022-21132

Risk Analysis		CVSS	Prioritization
Risk	**Medium**	**6.5** **Medium**	**Long.**
Impact	**Medium**		
Likelihood	**Likely**		
Hosts Impacted	Pfsense Wireguard 0.1.5 - 0.1.5_4		

Description
Directory traversal vulnerability. Allows a remote-authenticated attacker to lead a pfSense user to view a file outside the public folder. For Brick Wall Cyber, this means that an attacker could view sensitive files, such as internal company documents, or files from a client's backup network, depending on what device is affected.

External References
https://www.cve.org/CVERecord?id=CVE-2022-21132 https://nvd.nist.gov/vuln/detail/CVE-2022-21132

4.m CVE-2019-9510

Risk Analysis		CVSS	Prioritization
Risk	**Medium**	**7.8** **High**	**Short.**
Impact	**Medium**		
Likelihood	**Likely**		
Hosts Impacted	Remote File Server		

Description

A vulnerability in Microsoft Windows 10 1803 and Windows Server 2019 and later systems can allow authenticated RDP-connected clients to gain access to user sessions without needing to interact with the Windows lock screen. Should a network anomaly trigger a temporary RDP disconnect, Automatic Reconnection of the RDP session will be restored to an unlocked state, regardless of how the remote system was left. By interrupting network connectivity of a system, an attacker with access to a system being used as a Windows RDP client can gain access to a connected remote system, regardless of whether or not the remote system was locked.

A threat actor could gain access to an employee's remote file server by using a DOS attack to bypass the lock screen. This could reveal any sensitive information about clients networks that is stored on the remote file server.

External References
https://nvd.nist.gov/vuln/detail/CVE-2019-9510

4.n CVE-2019-0581

Risk Analysis		CVSS	Prioritization
Risk	**Low**	**7.8** **High**	**Evetl.**
Impact	**Medium**		
Likelihood	**Rare**		
Hosts Impacted	BWC's website, windows server 2012		

Description
A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory. This can cause any information accessible on BWC website to be accessed and the website can be changed, and/or taken down. While this is quite bad it is low risk due to the threat actor needing to have local access and be signed in, so unless other vulnerabilities were exploited or a worker was the threat actor this vulnerability has no risk.

External References

https://nvd.nist.gov/vuln/detail/CVE-2019-0581

4.o CVE-2023-34367

Risk Analysis		CVSS	Prioritization
Risk	**High**	**6.5 Medium**	**Short.**
Impact	**High**		
Likelihood	**Likely**		
Hosts Impacted	Employee workstations		

Description
Windows 7 is vulnerable to a full blind TCP/IP hijacking attack. Attackers could send commands to hosts on Brick Wall Cybers network remotely. The attacker could use this as a way to open up other vulnerabilities. Note: Microsoft believes this is too hard to pull off to be a real threat however cybersecurity professionals disagree.

External References
https://nvd.nist.gov/vuln/detail/CVE-2023-34367 https://portswigger.net/daily-swig/blind-tcp-ip-hijacking-is-resurrected-for-windows-7

4.p CVE-2024-0115

Risk Analysis		CVSS	Prioritization
Risk	**Medium**	**6.1 Medium**	**Long.**
Impact	**Medium**		
Likelihood	**Unlikely**		
Hosts Impacted	Kanboard, Ansible, ELK, Open VAS, GoPhish		

Description
A vulnerability in Python APIs where a user may cause an uncontrolled resource consumption issue by a long running CV-CUDA Python process. A successful exploit of this vulnerability may lead to denial of service and data loss. If an attacker has access to Brick Wall Cyber's network they could cause a DOS attack.

External References
https://nvd.nist.gov/vuln/detail/CVE-2024-0115