Vulnerability Assessment

December 3, 2022

REALLY
LEGIT
ELECTRONIC
SECURITY

An Assessment of:

Brick Wall Cyber

Security Assessment Team

Cayden Wright	Principal Analyst
Zachary Lineman	Security Analyst
Charlie Ives	Security Analyst
Hassan Alshehri	Security Analyst

Division of Responsibilities

<table>
<tr><th>Student</th><th>Expected Contributions</th></tr>
<tr><td>Cayden Wright</td><td>4 vulnerabilities + finalizing report + executive summary</td></tr>
<tr><td>Zachary Lineman</td><td>4 vulnerabilities + assistance in writing summaries</td></tr>
<tr><td>Charlie Ives</td><td>4 vulnerabilities + assistance in writing summaries</td></tr>
<tr><td>Hassan Alshehri</td><td>4 vulnerabilities + assistance in writing summaries</td></tr>
<tr><th colspan="2">Communication Plan</th></tr>
<tr><td colspan="2">Discord chat</td></tr>
<tr><th colspan="2">Meeting Schedule</th></tr>
<tr><td colspan="2">Talk after regularly scheduled class - otherwise, as necessary</td></tr>
</table>

1. EXECUTIVE SUMMARY

This summary is in regard to an assessment of Brick Wall Cyber (herein referred to as the “Client”) conducted by Really Legit Electronic Security, where the goal of R.L.E.S. was to assess the current security posture of the client’s computer systems, as well as provide recommendations to the Client on how to improve their security posture.

During the process of our assessment, R.L.E.S. found a myriad of vulnerabilities in BWC’s systems, and categorized them by risk into Critical, High, Medium, and Low. R.L.E.S. found a total of 3 Critical vulnerabilities, 10 High vulnerabilities, 4 Medium vulnerabilities, and 0 Low vulnerabilities. The Critical and High vulnerabilities render the client and their clients directly vulnerable to a breach of confidentiality, integrity, and/or availability, and must be remedied immediately. Medium and Low vulnerabilities, while still exposing BWC and its clients to attack, are less important and may be addressed after all Critical and High vulnerabilities have been fixed.

A majority of vulnerabilities in the Client’s systems fell into one of three categories. These categories include outdated software, misconfigured software, and ignorance of security best practices. While these are very broad categories that nobody can completely protect themselves from, it is imperative that the Client update and configure their software properly, as well as adhere to security best practices. Outdated software exposes BWC to a myriad of threats that are readily found, well-known, and easily exploited. Misconfigured software can be equated to leaving your front door unlocked: even if BWC had 100% effective security, misconfigured software can let attackers in through insecure protocols and methods. Disregarding security best practices such as password complexity is not immediately exposing the Client to cyber attacks; however, these best practices exist to mitigate common attacks and stop (or at least slow down) a cyber attack should it penetrate the other defenses of the Client.

R.L.E.S. recommends that the Client begin by addressing all Critical and High vulnerabilities by updating and reconfiguring all utilized software. While this certainly is a tall order, it is a small cost as compared to the thousands of hours (and dollars) required to recover from a cyber attack. After these are addressed, Medium and Low vulnerabilities should be remedied. Many of these will take a rather long time to fully implement, and it is advisable that the Client’s IT team take consistent, small steps to remedy these vulnerabilities. With a dedicated and responsive IT team, the remedies for all vulnerabilities present in our assessment should take no more than two calendar months.

2. THREATS AND RISK

2.a Threat Assessment

2.a.1 Threat Actor Motivations

Motivation	Relevance to Brick Wall Cyber
Money	Attackers could be after BWC (or their clients) to steal currency. BWC should ensure their financial assets (and those of their clients) are well protected
Ideology	Attackers could attack a client of BWC if said client does not align with their ideology.
Coercion	Someone could be coerced to attack BWC (or a client) by their boss/another adversary. An attacker could also attack BWC or a client to coerce them into following instructions from the attacker.
Ego	Attackers may attack BWC or their clients simply to say they did - or to prove their worth to a community

Motivation	Relevance to Brick Wall Cyber
Reciprocation	BWC or their clients may be attacked by someone who feels wronged by BWC or a client.
Authority	Similar to Coercion, an attacker may be attacking BWC or a client because they have been ordered to, or to show authority to that client/BWC.
Scarcity	Attackers could attack BWC or a client to obtain a resource that is scarce (money, computing time, IP, physical locations, etc)
Commitment / Consistency	Similar to Ideology, an attacker of BWC or a client could be motivated by staying consistent to a plan or social idea.
Liking	An attacker of BWC could be carrying out an attack to gain the favor of someone, whether it be a love or social interest, a boss, coworker, etc.
Social Proof	Similar to “Liking”, an attacker could be motivated to appear worthy among their peers.

2.a.2 Threat Model

Threat	High-level Mitigation	Importance for Brick Wall Cyber (Low/Medium/High)
Spoofing	Strong Authentication	High
Tampering	Strong authentication + authorization + logging	Medium
Repudiation	Stronger logging and encryption	High
Information Disclosure	Stronger encryption and tighter authentication	High
Denial of Service	Redundant systems and intelligent detection of attacks	Low
Elevation of Privilege	Find and repair vulnerable software	Medium

2.b Risk Matrix

RISK MATRIX		THREAT IMPACT			
LIKELIHOOD		LOW	MEDIUM	HIGH	CRITICAL
	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.)	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 discloses Personally Identifiable Information, Sensitive Information, or information that can lead to further access to sensitive data. 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 Most software is several years out of date

It is apparent to our firm that Brick Wall Cyber utilizes a plethora of out-of-date software, prevalent across the network, including but not limited to pfSense, ISC Bind, Wordpress, Docker, MariaDB, and more. Running such out-of-date software (sometimes by several years) is a gigantic security risk, as vulnerabilities are always being found (and not patched) for old software.

3.a.2 Several misconfigurations lead to use of vulnerable protocols

Brick Wall Cyber operates several different softwares which are misconfigured, allowing insecure and dangerous protocols including but not limited to SMB 1.0, SSL, and TLS 1.1. While this configuration does lead to increased compatibility with older software, it opens a significant portion of BWC to attack. For this reason, compatibility is not a valid excuse for BWC to use in this situation.

3.a.3 Several “Best Practices” not adhered to

Security is not always a technical issue. Through our audit of Brick Wall Cyber, R.L.E.S. has found that several security best practices as defined by NIST and other organizations have not been abided by, including password length, user privileges, up-to-date software and more.

3.b. Key Recommendations

3.b.1 Better manage software update process

After learning of the amount of out-of-date software that BWC utilizes, our firm strongly recommends that BWC monitors for new versions of software that it is using. They should then test it to ensure it is compatible with their needs, then deploy it to avoid being vulnerable to hundreds of software vulnerabilities. Perhaps it is best to delegate a team or time of week to software updates.

3.b.2 Review software configurations

Our firm recommends that for every software that Brick Wall Cyber operates, there must be a review of the relevant configuration files or settings, and any misconfigurations must be corrected. It is apparent to our firm that several softwares are configured improperly, allowing for a variety of attacks to be carried out against BWC or clients.

3.b.3 Adhere to best practices as defined by security agencies

It is imperative that BWC adheres to all security best practices. In our audit, we discovered several not being obeyed, such as password complexity and user privileges. BWC must consistently stay up-to-date with the latest security bulletins and best practices, and apply them to their organization as soon as possible

3.c. Response Plan

Mitigation Prioritization	Vulnerability
Immediate (Imme.)	● ISC Bind RCE Exploit ● MariaDB RCE Exploit ● Kernel Vulnerability in CentOS 6.9 ● Docker Container Escape with Root Access ● OSSEC Log Vulnerability ● Microsoft IIS 5.0 Privilege vulnerability CVE-2008-0074 ● Sendmail 8.13.0 CVE-2006-0058 ● Employee workstation still using Windows 7/8 ● OSSIM 5.3.2 privilege dropping
Short-term (Short.)	● pfSense 2.2 - Multiple XSS exploits ● OpenVAS Manager SQL Injection ● SquirrelMail 1.4.17 CVE-2011-275 ● OpenSSH 7.9 CVE-2019-6111 ● Ansible 2.9 Exploit
Long-term (Long.)	● Support for Outdated SSL and TLS protocols ● Wordpress 5.2.2 CVE-2019-16217
Eventual (Evetl.)	

4. VULNERABILITIES

4.a pfSense 2.2 - Multiple XSS exploits

Risk Analysis		CVSS	Prioritization
Risk	**HIGH**	**6.8** **Medium**	**Short Term.**
Impact	**Medium**		
Likelihood	**Likely**		
Hosts Impacted	pfSense Router - 10.x.0.1		

Description
Multiple Cross Site Scripting (XSS) vulnerabilities exist in pfSense 2.2. This allows for arbitrary JavaScript to be passed in through parameters in several URLs. However, this requires a logged-in administrator, meaning that the attack would need to involve social engineering to get an administrator to click a malicious link. Solution is to simply update pfSense.

External References
https://www.exploit-db.com/exploits/36506 https://nvd.nist.gov/vuln/detail/CVE-2015-2295

4.b ISC Bind RCE Exploit - CVE-2021-25216

Risk Analysis		CVSS	Prioritization
Risk	HIGH	9.8 Critical	Imme.
Impact	CRITICAL		
Likelihood	Unlikely		
Hosts Impacted	DNS Server - 10.0.0.2		

Description
Out-of-bound read error in ISC Bind 9.12 allows for unauthenticated attackers to execute arbitrary code as the “bind” user through passing of a specially-crafted TKEY query. Simple solution is to update ISC Bind.

External References
https://nvd.nist.gov/vuln/detail/CVE-2021-25216 https://www.zerodayinitiative.com/advisories/ZDI-21-657/

4.c Support for Outdated SSL and TLS protocols

Vulnerability Name		CVSS	Prioritization
Risk	MEDIUM	N/A	Long Term
Impact	MEDIUM		
Likelihood	LIKELY		
Hosts Impacted	WWW, 10.0.0.5		

Description
WWW server supports outdated and vulnerable protocols such as SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1, and TLS 1.2. While it may be difficult or unreasonable to remove every single deprecated protocol, it is imperative that BWC remove support for at least SSL 2.0, SSL 3.0, TLS 1.0, and TLS 1.1.

External References
https://www.cloudflare.com/learning/ssl/why-use-tls-1.3/ https://www.cisa.gov/uscert/ncas/alerts/TA14-290A

4.d MariaDB RCE Exploit CVE-2016-6662

Risk Analysis		CVSS	Prioritization
Risk	**CRITICAL**	**10.0** **Critical**	**Imme.**
Impact	**CRITICAL**		
Likelihood	**LIKELY**		
Hosts Impacted	Wordpress - 10.0.0.9		

Description
Allows a local user to create arbitrary configs and bypass protection mechanisms - can be leveraged to allow for arbitrary code execution by setting malloc_lib. Easy fix is to update MariaDB.

External References
https://nvd.nist.gov/vuln/detail/CVE-2016-6662#vulnCurrentDescriptionTitle https://www.cvedetails.com/cve/CVE-2016-6662/

4.e OpenVAS Manager SQL Injection CVE-2014-9220

Vulnerability Name		CVSS	Prioritization
Risk	**HIGH**	**7.5** **Partial**	**Short Term**
Impact	**HIGH**		
Likelihood	**MEDIUM**		
Hosts Impacted	OpenVAS - 10.1.0.20		

Description
Allows an attacker to execute arbitrary SQL commands through the timezone parameter when submitting a modify_schedule OMP command. This is a trivial exploit for an attacker to perform and requires no authentication to exploit.

External References
https://www.cvedetails.com/cve/CVE-2014-9220/ https://nvd.nist.gov/vuln/detail/CVE-2014-9220

4.f Kernel Vulnerability in CentOS 6.9 CVE-2017-1000253

Risk Analysis		CVSS	Prioritization
Risk	High	7.2 High	Imme.
Impact	High		
Likelihood	Medium		
Hosts Impacted	DNS - CentOS 6.9 - 10.0.0.2		

Description
This vulnerability comes from an unpatched kernel vulnerability in the CentOS linux kernel. The vulnerability stems from how the kernel loads elf binaries. When they are loaded, memory is not allocated correctly and maps part of the binary into the gap between the stack and binary, which could allow an unprivileged user to escalate their privileges on the system.

External References
https://www.cvedetails.com/cve/CVE-2017-1000253/ https://nvd.nist.gov/vuln/detail/CVE-2017-1000253

4.g Docker Container Escape with Root Access CVE-2019-5736

Risk Analysis		CVSS	Prioritization
Risk	CRITICAL	9.3 CRITICAL	Imme.
Impact	CRITICAL		
Likelihood	LIKELY		
Hosts Impacted	Wordpress -10.0.0.9		

Description
There is a vulnerability in Docker versions before 18.09.2 which includes 18.04 which allows attackers to overwrite the host runc binary. This allows an attacker to gain code execution when runc is run next. Since runc is run with root privilege, the attacker has full control of the host system. This attack can be performed from inside of either an attacker compromised image or an existing image where the attacker can run commands as root. This attack combined with CVE-2016-6662 as earlier mentioned will allow for a user to run commands as root in MariaDB, using those permissions to take over the host system.

External References
https://www.cvedetails.com/cve/CVE-2019-5736/ https://unit42.paloaltonetworks.com/breaking-docker-via-runc-explaining-cve-2019-5736/ https://nvd.nist.gov/vuln/detail/CVE-2019-5736

4.h OSSEC Log Vulnerability CVE-2020-8445

Risk Analysis		CVSS	Prioritization
Risk	CRITICAL	10.0 CRITICAL	Imme.
Impact	CRITICAL		
Likelihood	LIKELY		
Hosts Impacted	All BWC Windows Systems		

Description
A vulnerability in the OS_CleanMSG function does not clean terminal control characters or newlines out of processed log messages. This means that an attacker can obfuscate events and execute commands when the logs are viewed through vulnerable terminal emulators. Because all windows systems on the network are running OSSEC, they are submitting un cleaned logs. If any one of these logs are viewed in a vulnerable terminal emulator, an attacker can remotely execute scripts.

External References
https://www.cvedetails.com/cve/CVE-2020-8445/ https://www.cve.org/CVERecord?id=CVE-2020-8445

4.i Microsoft IIS 5.0 Privilege Vulnerability CVE-2008-0074

Risk Analysis		CVSS	Prioritization
Risk	**HIGH**	**7.2** **HIGH**	**Imme.**
Impact	**HIGH**		
Likelihood	**UNLIKELY**		
Hosts Impacted	www-10.0.0.5		

Description
This vulnerability in www hosts which is Internet Information Services Local Privilege Elevation vulnerability in Microsoft Internet Information Services (IIS) 5.0 allows local users to gain privileges via unknown vectors related to file change notifications in the TPRoot, NNTPFile\Root, or WWWRoot folders.

External References
https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A538 https://www.cvedetails.com/cve/CVE-2008-0074/

4.j Wordpress 5.2.2 CVE-2019-16217

Risk Analysis		CVSS	Prioritization
Risk	**MEDIUM**	**4.3** **MEDIUM**	**Long.**
Impact	**MEDIUM**		
Likelihood	**UNLIKELY**		
Hosts Impacted	Wordpress -10.0.0.9		

Description
WordPress vulnerabilities, such as cross-site scripting and open redirection. Wordpress, a web blogging tool, was found to have several vulnerabilities. They enabled remote attackers to conduct multiple XSS and CSRF attacks, establish open redirects, poison cache, and bypass authorisation access and input sanitation.

External References
https://www.cvedetails.com/cve-details.php?cve_id=CVE-2019-16218 https://www.debian.org/security/2020/dsa-4599

4.k SquirrelMail 1.4.17 CVE-2011-275

Risk Analysis		CVSS	Prioritization
Risk	HIGH	6.8 MEDIUM	Short.
Impact	HIGH		
Likelihood	LIKELY		
Hosts Impacted	Mail - 10.0.0.4		

Description
Multiple cross-site request forgery (CSRF) vulnerabilities in SquirrelMail 1.4.17 allow remote attackers to hijack the authentication of unspecified users through vectors including (1) the empty trash implementation and (2) the Index Order (aka options order) page.

External References
https://www.cvedetails.com/cve/CVE-2011-2753/ https://access.redhat.com/errata/RHSA-2012:0103.html

4.l Sendmail 8.13.0 CVE-2006-0058

Risk Analysis		CVSS	Prioritization
Risk	HIGH	7.6 HIGH	Imme.
Impact	CRITICAL		
Likelihood	LIKELY		
Hosts Impacted	Mail - 10.0.0.4		

Description
In Sendmail 8.13.0, a signal handler race situation allows remote attackers to execute arbitrary code by setting timeouts in such a way that the Setjmp and Longjmp function calls are interrupted and unexpected memory locations are modified.

External References
https://www.cvedetails.com/cve/CVE-2006-0058/ https://support.avaya.com/elmodocs2/security/ASA-2006-078.htm

4.m Ansible 2.9 Exploit - CVE-2019-14904

Risk Analysis		CVSS	Prioritization
Risk	**High**	**7.3** **HIGH**	**Short.**
Impact	**Medium**		
Likelihood	**UNLIKELY**		
Hosts Impacted	Ansible - 10.1.0.50, 10.5.0.5		

Description
When setting the name for a Zone (VM) on the Solaris host, the zone name is checked by listing the processes on the remote machine. An attacker can change the name of the zone and execute arbitrary commands on the remote machine. There are no mitigations at this time. However, the attacker needs local access to the machine and therefore is unlikely.

External References
https://nvd.nist.gov/vuln/detail/CVE-2019-14904 https://www.cvedetails.com/cve/CVE-2019-14904/ https://access.redhat.com/security/cve/cve-2019-14904

4.n Employee workstations still using Windows 7/8

Risk Analysis		CVSS	Prioritization
Risk	**HIGH**	**N/A**	**Imme.**
Impact	**HIGH**		
Likelihood	**LIKELY**		
Hosts Impacted	Employee workstations running Windows 7/8		

Description
Microsoft has stopped rolling out security updates for Windows 7, 8, and 8.1, leaving those Operating Systems completely vulnerable for attack. Employees should immediately update to a version of Windows that has not reached end-of-life.

External References
https://www.microsoft.com/en-us/windows/end-of-support?r=1

4.o OSSIM 5.3.2 privilege dropping (CVE-2017-6972)

Risk Analysis		CVSS	Prioritization
Risk	HIGH	10.0 CRITICAL	Imme.
Impact	HIGH		
Likelihood	LIKELY		
Hosts Impacted	All machines with OSSIM 5.3.2 installed - 10.1.0.40, 10.5.0.2		

Description
There is an error in OSSIM versions before 5.3.7 where privilege dropping occurs and unnecessarily executes code as root, leaving the systems hugely vulnerable.

External References
https://www.cvedetails.com/cve/CVE-2017-6972/

4.p OpenSSH 7.9 CVE-2019-6111

Risk Analysis		CVSS	Prioritization
Risk	Medium	5.9 Medium	Short.
Impact	Medium		
Likelihood	Likely		
Hosts Impacted	SSH Jump - 10.0.0.22		

Description
In OpenSSH 7.9, the server chooses which files and directories to send to the client through cursory validation of the object name. A man-in-the middle attacker can change arbitrary files in the target directory and can manipulate its contents.

External References
https://www.cvedetails.com/cve/CVE-2019-6111/