Vulnerability Assessment

December 09, 2023

Brick Wall Cyber

Security Assessment Team

Melissa Burisky	Principal Analyst
Logan Maleady	Security Analyst
Aman Patel	Security Analyst
Jess Tang	Security Analyst

Division of Responsibilities

Student	Expected Contributions
Melissa Burisky	Section 2.a, 4 vulnerabilities (4.i - 4.l), 3.a.1, summary of results
Aman Patel	4 vulnerabilities (4a to 4d), key recommendation and finding, summary of results
Logan Maleady	4 vulnerabilities (4.e-4.h), key recommendation and finding, summary of results, key recommendation and finding, summary of results
Jess Tang	4 vulnerabilities (4.m-4.p), key recommendation and finding, summary of results
Communication Plan	
Video calls, SMS group chat	
Meeting Schedule	
12/03/2023, 12/08/2023	

1. EXECUTIVE SUMMARY

As a company that offers managed security services and penetration testing, it is important that Brick Wall Cyber's security infrastructure is robust and secure. In order to identify potential risks within their environment, Brick Wall Cyber has requested a vulnerability assessment to be carried out. The goal of the vulnerability assessment was to perform a threat assessment, risk analysis and identify vulnerabilities within Brick Wall Cyber's environment. Because of the nature of their work, Brick Wall Cyber wants the security teams to pay particular focus to three issues of concern: Brick Wall Cyber’s vulnerability to attacks on systems that are directly accessible from the Internet, the vulnerability of systems on which Brick Wall Cyber stores client data, and the vulnerability of systems that are used to access Brick Wall Cyber client environments.

There are some threats and risks our security infrastructure manages. We know there are some threat actor motivations. Their motivations for money, ideology, coercion and ego. Specifically such as reciprocation, authority, scarcity, commitment, liking and social proof. Our security infrastructure also follows the reasoning according to the threat models when it comes to identifying vulnerability. These threat models we use include spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege. We also use our risk model to determine the severity of threat for the vulnerability. We determine by identifying how likely the vulnerability is going to appear, how risky or threatening the vulnerability is and how much impact it is going to leave. We found that there were five critical vulnerabilities and examples such as OSSIM Privilege Dropping, HTTP Request/Response Smuggling, and Exposure of Sensitive Information to an Unauthorized Actor. What they all have in common is that they have a very high risk of being cyber attacked and how much impact they are going to have on the system. There’s 7 high vulnerabilities and 3 medium vulnerabilities and what they all have in common is that they have high risks but they leave a low to medium impact on the system. There’s one low vulnerability we found in the assessment and they leave a low risk to the system and don't really make a big impact to the system.

After the assessment the team compiled a list of three key findings, These three include Improving Software Updates, Insufficient Network Segmentation, and Vulnerabilities with certificates. Probably one of the most widespread of these key findings is the lack of updated or current software. A lot of the software and systems used by brick wall cyber has not been updated in a while some of the software is even discontinued which poses a threat to security as it doesn’t have

new security features. Moreover, the assessment sheds light on the interconnected nature of these key findings, emphasizing the need for a holistic approach to cybersecurity. The lack of updated software not only exposes vulnerabilities but also exacerbates the risks associated with certificate management and network segmentation. For instance, an outdated system may not support the latest encryption protocols required for secure communication, rendering the existing certificates less effective in ensuring data integrity and confidentiality. Certificates are essentially a way to verify that a website is a legitimate website and not a fake. The company faces issues with certificate vulnerabilities leading to attackers creating spoofs of the website and people losing their information due to this.

The team also assembled a list of three key recommendations for Brick Wall Cyber to initiate which includes updating software, Multi-factor Authentication, and Updating certificates. As aforementioned a lot of the software and systems are out of date so our top recommendation which we view as a top priority is updating these software and systems to eliminate the large security risks that they pose. The next recommendation revolves around implementing Multi-Factor Authentication into the systems. This way if any attacker somehow gained the credentials of an employee they would not be able to physically get into the system without their other forms of authentication. Finally the last recommendation is to fix the issues with certificates. If Brick Wall Cyber wants to be a trusted company then they need to have a secure website that everyone can access without worry of getting their information stolen or accidentally going to a fake version of the website that is essentially identical. By adopting a multifaceted approach, the organization can significantly strengthen its overall security resilience and better protect against potential cyber threats and attacks.

2. THREATS AND RISK

2.a Threat Assessment

2.a.1 Threat Actor Motivations

Motivation	Relevance to Brick Wall Cyber
Money	A threat actor motivated by money could attack Brick

	Wall Cyber for the purpose of gathering information about the company or their clients to sell. Brick Wall Cyber, as a security services company, has access to intricate details about their clients security systems, and of potential vulnerabilities or weaknesses in those systems. A threat actor could look to steal and sell that information to other potential threat actors, who could then use that information to attack the clients. This motivation is highly likely for potential threat actors of Brick Wall Cyber.
Ideology	A threat actor motivated by ideology could also attack Brick Wall Cyber if their ideology was threatened by a company such as Brick Wall Cyber or by any of their clients. The threat actor could attack Brick Wall Cyber to gain access to their client's private information, whether that be about their security system, potential vulnerabilities, or even billing information. The threat actor could then use that data to carry out further ideologically motivated attacks against the client. This motivation is likely for potential threat actors of Brick Wall Cyber.
Coercion	A threat actor motivated by coercion could attack Brick Wall Cyber if they were being forced to by another party, through blackmail or other means of coercion. The threat actor could also feel like they had no choice but to try and damage the company or steal information. This could be a result of a spurned client or employee, or other party that feels like Brick Wall Cyber or their clients have harmed them. This motivation is less likely for potential threat actors of Brick Wall Cyber.
Ego	An actor motivated by ego may attack Brick Wall Cyber to simply prove to themselves or others that they could. They see themselves as better than the company and carry out the attack to prove it. This could also be a case of a spurned client, employee, or other party. Also, the threat actor could also hold such sentiments towards Brick Wall Cyber's clients and use the company as a stepping stone to carry out attacks on their true target. This motivation is less likely for potential threat actors of Brick Wall Cyber.

Motivation	Relevance to Brick Wall Cyber

Reciprocation	A possible reciprocation pretext for Brick Wall Cyber would be an attacker having knowledge of some favor being carried out between employees, by means of listening to internal communications within Brick Wall Cyber. The attacker then pretends to be the employee who did the favor and messages the favor recipient, asking that the favor be returned by doing some action or sending privileged information.
Authority	A possible authority pretext for Brick Wall Cyber would be an attacker pretending to be an important person such as a client or senior management within Brick Wall Cyber, and asking the target to send results of a security analysis and penetration testing. If the target complies and sends the client information, the attacker could then use that to perform an attack on the client.
Scarcity	A possible scarcity pretext for Brick Wall Cyber would be an attacker attempting to bribe employees to send the personal or security information of Brick Wall Cyber or its clients. If the target agrees and sends the company or client information, the attacker could then use that to perform an attack on the Brick Wall Cyber or the client.
Commitment / Consistency	A possible commitment/consistency pretext for Brick Wall Cyber would be an attacker listening to internal communications at Brick Wall Cyber, waiting for an employee to send personal or client information. Then the attacker would message that employee asking, pretending to be the original recipient, asking them to send it again, noting that they sent it once and can easily send it again.
Liking	A possible liking pretext for Brick Wall Cyber is an attacker pretending to be a significant figure within Brick Wall Cyber or the client organization. The attacker asks the target to send privileged information or do some other action, on the basis that they will be “liked” or in the good graces of the supposed figure.
Social Proof	A possible social proof pretext for Brick Wall Cyber would be pretending to be a significant figure within Brick Wall Cyber. The attacker would ask the target to send privileged information or do some other action, on the basis that they will receive some boast-worthy reward such as a company-wide kudos or other recognition within Brick Wall Cyber.

2.a.2 Threat Model

Threat	High-level Mitigation	Importance for Brick Wall Cyber (Low/Medium/High)
Spoofing	Authentication Controls: - Multi-factor authentication Preventative Controls: - Packet filtering firewalls Administrative Controls: - Organizational policy - Employee compliance testing (GoPhish)	High
Tampering	Integrity Controls: - System monitoring - Centralized logging - SIEMS Authentication Controls: - Multi-factor authentication Authorization Controls: - Access controls - System isolation	High
Repudiation	Accountability Controls: - Centralized logging - System monitoring - Digital signatures	Medium
Information Disclosure	Confidentiality	High

	Controls: - Access controls - VPNS - Firewalls - Encryption Authentication Controls: - Multi-factor authentication	
Denial of Service	Availability Controls: - System redundancy - Recovery sites (hot/warm sites)	Medium
Elevation of Privilege	Authorization Controls: - Access controls - System isolation Authentication Controls: - Multi-factor authentication	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 leaks 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 Improve Software Update Processes

Many of the vulnerabilities found in Brick Wall Cyber's infrastructure involve old and outdated software being limited in functionality and susceptible to attacks. In addition, a number of these vulnerabilities are prioritized as immediate, meaning that the finding has a critical impact on the company or their clients. Examples of such outdated software within the Brick Wall Cyber infrastructure include OpenSSH, where the host SSH Jump has version 7.9. This version of OpenSSH is vulnerable to a man-in-the-middle attack, during which the attacker could manipulate files and directories. This host is used by BWC administrators to access their systems from home, meaning that if SSH Jump is compromised using this vulnerability then all accessed systems will be compromised as well. In addition, the majority of the logging software, such as Logstash and Kibana, used by Brick Wall Cyber are massively outdated, and again have major vulnerabilities present. There are many other examples of outdated software in Brick Wall Cyber's infrastructure that present vulnerabilities. Brick Wall Cyber needs to review the current versions of their used software and make efforts to download the most up-to-date versions regularly to rectify issues and mitigate potential attacks.

3.a.2 Insufficient Network Segmentation

A key finding in Brick Wall Cyber's vulnerability assessment is the presence of insufficient network segmentation, allowing potential attackers to move laterally within the network. This lack of segmentation means that once an attacker gains access to a specific part of the network, they have the potential to traverse and compromise other critical systems and data. This finding poses a significant risk to the confidentiality and integrity of sensitive information stored within the network. To address this, Brick Wall Cyber should implement a robust

network segmentation strategy, dividing the network into distinct segments with appropriate access controls, reducing the lateral movement capability of attackers.

3.a.3 Certificates Vulnerability

Our key finding related to certificates vulnerability is that cyber attacks related to expired CA are increasing. This happens because when your certificate expires, your website is no longer proving that it's a real website. This can cause problems where data is more likely going to be leaked in man in the middle attacks and where your data can be stolen in the attack. This also can lead to increase in vulnerability and lead to Denial of Service attacks (DOS) for websites. Another thing is that it allows spoofing or attackers to lead people thinking it's a website, but instead it's for people to confine themselves leading to their data being stolen.

3.b. Key Recommendations

3.b.1 Update software as soon as possible

As mentioned in 3.a.1 Improve Software Update Processes Brick Wall Cyber consists of a lot of outdated software. The vulnerabilities created by these vulnerabilities pose a way greater risk than any potential down time / loss of revenue that might be associated with updating their systems. The best thing to do is to create and implement a plan for updating all the outdated software and systems. This plan should likely consist of three phases, the preparation phase, the update phase, and the configuration phase. The preparation phase would consist of backing up any data or systems that may be affected. The update phase which would consist of updating the software likely in waves such that everything is not shut down all at once. The final phase would involve reconfiguring any systems that need them, installing new software on updated machines, and recovering any data that needs to be recovered from the backups.

3.b.2 Multi-Factor Authentication (MFA)

By requiring users to present multiple forms of identification before gaining access, MFA is intended to improve the security of digital accounts and systems. Using a combination of the user's knowledge (password), possessions (mobile device, security token, smart card), and identity (biometric data, such as fingerprints or facial recognition), multi factor authentication MFA adds an extra degree of security. This multi pronged strategy greatly reinforces authentication procedures, increasing the difficulty with which unauthorized parties can obtain sensitive data. In the end, MFA contributes to a more robust and resilient security posture for both individuals and organizations by preventing unauthorized access, lowering the risk of identity theft, and protecting against various cyber threats.

3.b.3 Update Certificate Vulnerabilities

The solution to the problem is that every website or application should always update or renew their CA certificate to ensure that their website is protecting their own data and proving that it’s in their website. Every website wants to make sure that the users’ data is being protected as they are entering into each website and application, without worrying about their data being attacked. They can always update their servers certificate by using SHA-256 rather than SHA-1, because SHA-256 is newer and has better security features than SHA-1 as they’re old and outdated, leaving the website vulnerable.

3.c. Response Plan

Mitigation Prioritization	Vulnerability
Immediate (Imme.)	• Outdated Version of OpenSSH • Windows 7 and 8 Support • Logstash Malformed URLS Sensitive Data Disclosure • OSSIM Privilege Dropping • Improper Handling of Certificates

	• Exposure of Sensitive Information to an Unauthorized Actor • HTTP Request/Response Smuggling
Short-term (Short.)	• Weak Email Passwords • Kibana xpack.security.audit.enabled Setting • Change in Public Key Authentication • SHA-1 Hash Algorithm • Improper Input Validation • Argument Injection
Long-term (Long.)	• Admin privileges on Corporate Workstations • Kanboard Missing Access Control • DoS Attack
Eventual (Evetl.)	

4. VULNERABILITIES

4.a Change in Public Key Authentication

Risk Analysis		CVSS	Prioritization
Risk	**Low**	**3.7 Low**	**Short.**
Impact	**Low**		
Likelihood	**Likely**		
Hosts Impacted	OpenSSH 8.0		

Description
If a client is using public key authentication, and an attacker modified the server, then the user can't determine if the authentication can confirm that he can connect to a right server or is it going to connect to the unwanted server.

External References
https://www.cvedetails.com/cve/CVE-2021-36368/

4.b DOS Attack

Risk Analysis		CVSS	Prioritization
Risk	**High**	**7.5 High**	**Long.**
Impact	**Low**		
Likelihood	**Very Likely**		
Hosts Impacted	OpenSSH 8.0		

Description

Attackers caused denial of service by sending the server under the attacker's control and the server wouldn't respond but send excessive amounts of data or does nothing after TCP handshake. The attacker got the control by getting the intermediate CA certificate.

External References
https://www.cvedetails.com/cve/CVE-2022-40617/

4.c Improper Handling of Certificates

Vulnerability Name		CVSS	Prioritization
Risk	**High**	**7.5 High**	**Imme.**
Impact	**Low**		
Likelihood	**Likely**		
Hosts Impacted	Windows Server 2019, Windows Server 2012		

Description
It's where we place CA certificates into Trusted Root certificates and we publish private key into a file in public software distribution, but unfortunately we allow the attackers to perform spoofing the websites leading people to think it's a real website but it's not. So these certificates need to be avoided.

External References
https://www.cvedetails.com/cve/CVE-2018-17612/

4.d SHA-1 Hash Algorithm

Risk Analysis		CVSS	Prioritization
Risk	**High**	**7.8**	**Long.**
Impact	**5.9**		

Likelihood	**Likely**	**High**	
Hosts Impacted	OpenSSH, websites, mail		

Description
A person used SHA-1 hash for password storage, in which it's easy for attackers to guess the password easily. The attackers apparently used unsafe malware and applied it on the victim. SHA-1 was never recommended for password storage or even for certificates, it's unsafe and out of date. Websites and passwords using SHA-1 certificates are more likely to put their data at risk and applying malware to their data.

External References
https://docs.digicert.com/en/certcentral/certificate-tools/discovery-user-guide/tls-ssl-certificate-vulnerabilities/sha-1-hashing-algorithm.html https://cvedetails.com/cve/CVE-2018-9233/

4.e Weak Email Passwords

Risk Analysis		**CVSS**	**Prioritization**
Risk	**High**	**N/A** **High**	**Short.**
Impact	**High**		
Likelihood	**Likely**		
Hosts Impacted	Mail, potentially more		

Description
Passwords have a minimum of 6 characters and must have upper and lowercase letters. This creates an issue because a 6 character password can be cracked in seconds especially since there are no special characters and only alphabetical characters. Passwords should be twice as long in length and require numbers and special characters. An attacker gaining access to an email could potentially send malware through email from what looks like a trusted account or obtain sensitive information using this email account.

External References

https://www.komando.com/security-privacy/check-your-password-strength/783192/#:~:text=Even%20if%20you%20use%20all,characters%20will%20take%20mere%20seconds.

4.f Outdated Version of OpenSSH

Risk Analysis		CVSS	Prioritization
Risk	**High**	**5.9 Medium**	**Imme.**
Impact	**High**		
Likelihood	**Unlikely**		
Hosts Impacted	SSH Jump and all hosts accessed by SSH Jump		

Description
The scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A Man-in-The-Middle attacker could overwrite arbitrary files in the scp client target directory. If recursive operation is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).This attack is unlikely because of the complexity of the attack and potential variables that the attacker can't control

External References
https://nvd.nist.gov/vuln/detail/CVE-2019-6111 https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?name=CVE-2019-6111&vector=AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N&version=3.1&source=NIST

4.g Windows 7 and 8 Support

Risk Analysis		CVSS	Prioritization
Risk	**Critical**	**7.5 High**	**Imme.**
Impact	**Critical**		
Likelihood	**Very Likely**		
Hosts Impacted	Corporate, Anything on these workstations		

Description
Windows 7 and 8 are no longer supported by microsoft which means any vulnerabilities and bugs that arise will not necessarily be fixed. This could lead to huge data leaks and exposure of information from BrickWall Cyber's systems and could allow attackers to potentially gain access to other systems from these machines. Since 2020 When Windows 7 stopped being supported there have been 1011 Vulnerabilities with an average CVSS of 7.55

External References
https://www.zdnet.com/article/windows-7-end-of-life-security-risks-and-what-you-should-do-next/ https://stack.watch/product/microsoft/windows-7/#:~:text=June%2014%2C%202023-,Windows%207%20is%20vulnerable%20to%20a%20full%20blind%20TCP%2FIP,(including%20many%20IoT%20devices).

4.h Admin privileges on Corporate Workstations

Risk Analysis		CVSS	Prioritization
Risk	**Medium**	**N/A** **Medium**	**Long.**
Impact	**Medium**		
Likelihood	**Unlikely**		
Hosts Impacted	Corporate, Workstations		

Description
Users have privileges to install software and configure their own systems as needed. The issue with this is that in the situation where an employee fell victim to something like a phishing attack and were prompted to download something they would be able to potentially download and install malicious software onto their systems. All Installs should be at the very least reviewed and approved by Internal IT/OPS

External References
Should You Allow Your Staff To Install Software?

4.i Logstash Malformed URLS Sensitive Data Disclosure

Risk Analysis		CVSS	Prioritization
Risk	**Critical**	**9.8 Critical**	**Imme.**
Impact	**Critical**		
Likelihood	**Likely**		
Hosts Impacted	ELK (10.1.0.60) - Logstash version 1.4.2 ELK (10.5.0.3) - Logstash version 1.4.2 Ansible (10.5.0.5) - This system is used to remotely configure all new client systems with log analysis with ELK		

Description
A sensitive data disclosure flaw was found in the way that Logstash versions before 5.6.15 and 6.6.1 logs malformed URLs. If a malformed URL is specified as part of the Logstash configuration, the credentials for the URL could be inadvertently logged as part of the error message.

External References
https://nvd.nist.gov/vuln/detail/CVE-2019-7612 https://www.elastic.co/community/security

4.j Kibana xpack.security.audit.enabled Setting

Risk Analysis		CVSS	Prioritization
Risk	**High**	**9.0 Critical**	**Short.**
Impact	**High**		
Likelihood	**Likely**		
Hosts Impacted	ELK (10.1.0.60) - Logstash version 1.4.2 ELK (10.5.0.3) - Logstash version 1.4.2 Ansible (10.5.0.5) - This system is used to remotely configure all new client systems with log analysis with ELK		

Description
Kibana versions before 6.6.1 contain an arbitrary code execution flaw in the security audit logger. If a Kibana instance has the setting xpack.security.audit.enabled set to true, an attacker could send a request that will attempt to execute javascript code. This could possibly lead to an attacker executing arbitrary commands with permissions of the Kibana process on the host system.

External References
https://nvd.nist.gov/vuln/detail/CVE-2019-7610 https://discuss.elastic.co/t/elastic-stack-6-6-1-and-5-6-15-security-update/169077

4.k Kanboard Missing Access Control

Risk Analysis		CVSS	Prioritization
Risk	**Medium**	**6.5** **Medium**	**Long.**
Impact	**Medium**		
Likelihood	**Very Likely**		
Hosts Impacted	Kanboard (10.1.0.30) - Kanboard version 1.2.7		

Description
Kanboard is open source project management software that focuses on the Kanban methodology. A vulnerability related to a missing access control was found, which allows a user with the lowest privileges to leak all the tasks and projects titles within the software, even if they are not invited or it's a personal project. This could also lead to private/critical information being leaked if such information is in the title. This issue has been addressed in version 1.2.30. Users are advised to upgrade. There are no known workarounds for this vulnerability.

External References
https://nvd.nist.gov/vuln/detail/CVE-2023-33970

4.l OSSIM Privilege Dropping

Risk Analysis		CVSS	Prioritization
Risk	**Critical**	**9.8 Critical**	**Imme.**
Impact	**Critical**		
Likelihood	**Likely**		
Hosts Impacted	OSSIM (10.1.0.40) - OSSIM version 5.3.2 OSSIM (10.5.0.2) - OSSIM version 5.3.2 Ansible (10.5.0.5) - This system is used to remotely configure all new client systems by installing monitoring permit incident monitoring with OSSIM/OSSEC.		

Description
AlienVault USM and OSSIM before 5.3.7 and NfSen before 1.3.8 have an error in privilege dropping and unnecessarily execute the NfSen Perl code as root, aka AlienVault ID ENG-104945. A remote authenticated attacker (or an attacker with a stolen PHP Session ID) can gain complete control over the system by sending a crafted request with shell commands which will be executed as root on a vulnerable system. The commands are executed as root due to CVE-2017-6972

External References
https://nvd.nist.gov/vuln/detail/CVE-2017-6972 https://www.exploit-db.com/exploits/42314

4.m Argument Injection

Risk Analysis		CVSS	Prioritization
Risk	**High**	**7.7 High**	**Short.**
Impact	**5.5(Medium)**		
Likelihood	**0.04%(Unlikely)**		
Hosts Impacted	Jellyfin (videoCodec and audioCodec)		

Description
Jellyfin, a Media System for media streaming, discovered a security vulnerability in its VideosController affecting certain endpoints. This flaw, present in the current version, allows unauthenticated access, but exploiting it is challenging due to the need to guess a random GUID. The vulnerability involves argument injection in query parameters, potentially impacting the FFmpeg command line. Upgrading to version 10.8.13 addresses the issue, and users are urged to update, as no workarounds are available.

External References
https://nvd.nist.gov/vuln/detail/CVE-2023-49096 https://www.cvedetails.com/cve/CVE-2023-49096/

4.n Improper Input Validation

Risk Analysis		CVSS	Prioritization
Risk	**High**	**8.2** **High**	**Short.**
Impact	**4.2(Medium)**		
Likelihood	**0.07%(Unlikely)**		
Hosts Impacted	Qlik Sense Enterprise		

Description
A path traversal vulnerability in Qlik Sense lets a remote, unauthorized attacker establish an anonymous session by submitting specially constructed HTTP requests. The attacker might be able to send more requests to unapproved endpoints during this anonymous session.

External References
https://www.cvedetails.com/cve/CVE-2023-41266/

4.o HTTP Request/Response Smuggling

Risk Analysis		CVSS	Prioritization
Risk	**Critical**	**9.6 Critical**	**Imme.**
Impact	**5.8(Medium)**		
Likelihood	**0.08%(Unlikely)**		
Hosts Impacted	Qlik Sense Enterprise		

Description
A remote attacker can elevate their privilege by tunneling HTTP requests in the raw HTTP request due to an HTTP Request Tunneling vulnerability found in Qlik Sense Enterprise for Windows versions May 2023 Patch 3 and earlier, February 2023 Patch 7 and earlier, November 2022 Patch 10 and earlier, and August 2022 Patch 12 and earlier. This enables users to submit requests that are processed by the repository application's backend server.

External References
https://www.cvedetails.com/cve/CVE-2023-41265/

4.p Exposure of Sensitive Information to an Unauthorized Actor

Risk Analysis		CVSS	Prioritization
Risk	**Critical**	**10.0 Critical**	**Imme.**
Impact	**6.0(High)**		
Likelihood	**51.75%(Very Likely)**		
Hosts Impacted	ownCloud owncloud/graphapi GetPhpInfo.php		

Description
In ownCloud owncloud/graphapi 0.2.x prior to 0.2.1 and 0.3.x prior to 0.3.1, a problem was found. A third-party GetPhpInfo.php library is used by the graphapi app to supply a URL. The PHP environment's configuration details can be seen by visiting this URL (phpinfo). The webserver's environment variables are all included in this data. Sensitive information like the license key, mail server credentials, and ownCloud admin password may be included in these environment variables in containerized deployments. The vulnerability persists even after you disable the graphapi app. Furthermore, phpinfo makes available a number of other potentially sensitive configuration details that an attacker could use to learn more about the system.

External References
https://www.cvedetails.com/cve/CVE-2023-49103/ https://owncloud.com/security-advisories/disclosure-of-sensitive-credentials-and-configuration-in-containerized-deployments/