Threat Assessment

Client:Artemis Inc.

	Description	Operating system	Risk of Exploit	Risk	Remediation	Action
1	**Unpatched RDP is exposed to the internet**	Windows OS	**High-** Network can be acessed and controlled remotely via brute force of password, installing malware and possibly ransomware.	CVSS 7.6	Patch RDP and configure settings.	Provide access list to trusted IP list only and close list, eliminate admins access, network level authentication and high
	Allow attackers access to an entire network, giving an entry point					
2	**web application is vulnerable to SQL**	Windows/Linux OS	**High**-Actors use malicious code to manipulating database and stealing all data.	CVSS 7.6	Using paratermized queries, typed parameters and stored proceedures.	Update all servers and software, use principal of least priveledge, provide stored list of proceedures and seperate any shared database accounts between web sites and applications.
	Through the SQL Oracle database, can be used to access unauthorized data.					
3	**Default password on Cisco admin portal**	Linux OS	**Medium-**Easy attack to network and gain admin rights to exploit system and access data.	CVSS 7.1	Change default password	Reconfigure the switch and change admin username and password .
	Password can be assessed remotely, by unathenticated adversaries.					
4	**Apache web server vulnerable to CVE-2019-0211**	Linux/Unix OS	**High**-Attacker gaining root access by running a script.Root access can allow access to all files shared.	CVSS 7.9	Upgrade apache	Upgrade to Apache 2.4.39 version.
	Unprriveledge scripts can be executed and main apache process at risk.					
5	**Web server is exposing sensitive data**	Linux OS	**Medium-**Attackers access data via the company inadvertly exposing information, allowing an attack.	CVSS 6.7	Ensure strong alogrithms and keys are used as well as proper key management.	create a comprehensive security policy, store sensitive data securely and properly dispose sensitive data.
	Organization unknowingly exposes sensitive data, causes risk of attack.					
6	**Web application has broken access control**	Linux/Windows OS	**Medium-**Access permissions are misfigured, allowing actors to gain access to financial records & data.	CVSS 5.4	Access validation controls	Audit and test access control, deny access by default and seperate access by resource
	Users accessing some resources or performing unauthorized functions.					
7	**Oracle WebLogic Server vulnerable to CVE-2020-148**	Linux OS	**High**-Attacker makes access remotely, to perform traversal attacks to compromise oracle.	CVSS 8.0	Encryption and using a file system.	Enable SSL in web logic and secure file system on deployment, limiting directory and file access.
	Unauthenticated attacker with network access via HTTP to compromise Oracle.					

8	**Misconfigured cloud storage (AWS security group misconfiguration, lack of access restrictions)**				Configure cloud environment	Configure cloud via AWS system.
	Cloud based system not configured correctly, allowing access to hackers.	**Linux OS Medium -** Attacker can gain access to storage buckets,cloud based data and install a skim code, to gain access to credit cards, social security numbers, addresses and phone numbers.		CVSS 7.6		
9	**Microsoft Exchange Server vulnerable to CVE-2021-26855**	Windows OS	**High-**	Attacker induces server side of application, to allow access or modify resources, such as 3rd party URL control.		
	SSRF, allowing external actor to send HTTP requests and authenticate to internal servers.			CVSS 8.4	Develop a whitelist and idetification.	Develop a whitelist of DNS domains, disable URL's and internal authentification.
	****Threat assessment process will take an estimated 2 days**					
	Reference: CVSS Calculator version 3.1 https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator					