VULNERABILITY	DESCRIPTION OF VULNERABILITY	OS/VERSIONS AFFECTED	RISK OF EXPLOITING	SUCCESSFUL EXPLOITATION RISK	REMEDIATION ACTION	CVSS SCORE
Unpatched RDP	Unpatched (Remote Desktop Protocol) RDP is exposed to the internet. RDP is used by the Windows client to connect directly to the Window server's operating system. From that connection, a user can open directories, download and upload files, and run programs on the server. An attacker can connect to the server from the internet as administrator if there is a RDP vulnerability. After the attacker gains access to the server, they can perform reconnaissance on the entire IT infrastructure.	Microsoft Windows Clients and Servers (NT and later)	RDP is a network protocol therefore the pen tester runs the risk of consuming network bandwidth during the exploitation phase.	Upon successfull RDP exploitation of the Windows Server hosting the Active Directory, the pentester can: 1. gain information of the domain such as domain name, users, groups, Organizaional Units. In addition, the pentester 2. find out that Artemis uses Microsoft Exchange server, and uses SSO to authenticate to the SAP ERP application 3. look at the Event Log to find out when the Windows services are used by the clients. 4. download and install programs 5. disable security software 6. erase backups and disable scheduled backups	Artemis needs to take the following remediation: 1. stop connecting directly to their servers over the internet 2. disallow external connections from the internet to local machines on the intranet on port 3389 (RDP port) at the perimeter firewall/DMZ 3. test and deploy patches for the RDP vulnerability and enable Network Level Authentication 4. install two-factor authenticaton (2FA) 5. install a virtual private network (VPN) gateway between RDP connections and internet 6. replace/upgrade insecure computer 7. for the accounts that use RDP, require the users to use long and complex passwords	9.2 Critical
SQL Injection	Web application is vulnerable to SQL injection. The web application at Artemis is hosted on a Windows Server. The application was developed using a scripting language that connects to the Oracle Datablase hosted on Linux. SAP used as the Enterprise resource planning (ERP) solution at Artemis is also hosted on the Linux servers.	Oracle 12c	The pentester will use Burp Suite for fuzzing to test for the SQL injection vulnerabilites. This might cause network and CPU bottleneck if the payload consists of thousands of entries in the file.	Upon successfull SQL injection exploitaton of the Oracle database, the pentester can: 1. obtain sensitive information of the Artemis customers such as names, addresses and credit card numbers resulting in a data breach and reputational damage 2. obtain Personal Identifcaion Information (PII) of the employees such as names, addresses, date of birth and Social Security number 3. update or delete data in the tables of the customer and employee databases	Artemis needs to take the following remediation actions to prevent SQL Injections: 1. Use prepared statements in the SQL code in oracle. The parameters to prepared statements don't need to be quoted. One of the first actions an attacker will perform to check for successfull SQL injections is use a singe quote in their input. If the backend does not sanitize the input, a syntax error will occur. 2. Use stored procedures. Stored procedures are pre-compiled. This prevents SQL injections since no matter what the user provides, it can't alter the underlying SQL statement.	9.7 Critical
Default Password	Default passwords are intended for initial testing, installation and configuration operations, however,the default password is still being used on the Cisco admin portal. Attackers can easily obtain default passwords and identify internet-connected target systems. Passwords can be found in product documentation and compiled lists available on the internet. Search engines such as Shodan can expose the systems at Artemis if the Cisco router is compromised.	Most Cisco routers and switches (model numbers starting with ESW, RV, SF, SFE, SG, SGE, SLM, SPA, SRP, SRW, WRP, and WRV.	The pentester can use a password-cracking tool that supports a wide range of network protocols such as THC Hydra. This tool used a file with a word-list of all possible passwords to perform a brute-force attack on the default passwords of network routers. If there is a rate limit on the target service to prevent brute-force attacks, then account lockouts will occur and the attack will fail.	Upon discovering the default password on the Cisco admin portal, the pentester can: 1. compromise all systems connected to the router leading to data breaches 2. can upload a worm (a stand-alone malicious program) which can then self-replicate and propagate separately. The worm that is uploaded can be similar to Stuxnet which targets SCADA in Industrial Control Systems.	Artemis needs to take the following remediation steps to prevent the network administrators from using the default Cisco router: 1. change the default passwords as soon as possible 2. allow internet access to mandatory network services and do not utilize systems that can be directly accessed from the internet. 3. Phase out the cisco routers and use FortiGate routers. In Fortios 6.2.1 and later, adding a password to the admin administrator is mandatory. The user will be prompted to configure it the first time they log in to FortiGate using that account, after a factory reset, and after a new image installation.	9.3 Critical
Apache Web Server (CVE-2019-0211)	Apache Web Server is vulnerable to CVE-2019-0211. When the system loads mod_php as an Apache module (software that enhances the performance of Apache HTTPD server), it allows Apache to interpret PHP files. The vulnerability makes it possible for mode_php to run code with the priveleges of the parent process which is primarily root.	Apache HTTP Server 2.4 releases 2.4.17 - 2.4.38	The pentester is at risk for logging in as Apache user and escalating to root. As root user, they will unintentially compromise the system.	After logging in as apache user, the pentester uses mod_php to run code with the priveleges of root. They will change the mod_php module and run malicious code.	Artemis needs to take the following remediation steps to prevent the mod_php module from running code with the privileges of root: 1. Patch the Apache software. 2. By default apache processes are either owned by "apache" or "nobody". The "nobody" userid and group that comes default on UNIX variants should not be used to run the web server. The "nobody " account was formerly introduced as a means to map the "root" account over NFS. Due to the associaton between the "nobody" and "root" accounts, new accounts should be created to run the web server.	6.7 Medium
Sensitive Data Exposure	The web server is exposing sensitive data. The web server is Windows server 2019 running Internet Information Services (IIS) and Active Directory. The data exposed is either data at rest or data in transit.	Windows Server 2019 IIS Active Directory	The pentester will capture username and passwords in clear text when they use wireshark to examine data in transit. Data at rest is captured using Burp suite and will also contain username and passwords in clear text.	Upon successfully capturing sensitive day in rest and in transit, the penteseter/threat actor will perform the following: 1. access usernames and passwords to compromise the systems at Artemis 2. access personal identifiable information (PII) such as names, addresses, date of birth, and social security numbers of customers resulting in Artemis's loss of reputation. 3. publish credit card numbers on the dark web	Artemis needs to take the following remediation steps to lower the risk of exposing sensitive data on the web server: 1. Classify data and identify which data is sensitive which would allow the Oracle DBA's to encrypt the columns containing the sensitive data at rest. 2. Don't store sensitive data unnecessarily. 3. Use proper and secure key management. 4. Encrypt data in transit with TLS and secure parameters such as forward secrecy ciphers. In addition, enforce encryption using HTTP Strict Transport Security (HSTS). 5. Do not use insecure legacy protocols for data in transit such as FTP, Telnet, and SMTP.	6.6. Medium
Broken Access Control	The web application hosted on Windows Server and using IIS has broken access control for users on the website. Access control is a set of policies given to users that prevents them from acquiring escalated permissions outside of their intended permissions.	Windows Server 2019 IIS Active Directory	The pentester/attacker will change the URL of the Artemis home page to force browsing to sensitive web pages. If an unauthenticated user can access either page, it's a flaw. If a non-admin can access the admin page, then is also a flaw.	Upon successfully browsing the Artemis website and accessing web pages with no authentication requirements, the pentester will access an admin page that contains application information. They will then have access to the company's IP addresses, hostnames, network devices and even usernames.	Artemis needs to take the following remediation steps to lower the risk of broken access control vulnerabilites: 1. since a new IIS website by default is open to everyone with anonymous access enabled, the administrator will need to enable Windows Authentication and disable Anonymous access. 2. Break inheritence on the website and remove the generic domain user "Users" from having access to it. 3. For specific pages in the website, add a group and configure permissions such as read only access. Add users to this group which will then give read access to that particular page. 4. To keep users permissions organized, do not check "include inheritable permissions from this objects parent" from this particular page.	7.5 High
Oracle WebLogic Server (CVE-2020-14882)	CVE-2020-14882 references a remove code execution vulnerability on Oracle WebLogic Server. The Oracle Weblogic application server centralizes and manages all services consisting of web server functionality, business components, and access to backend enterprise systems.	Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0	Since this is a remote code execution vulnerability, the arbitrary code the pentester executes will compromise the system.	Upon successful exploitation of this vulnerability, the unauthenticated threat actor will achieve remote code execution on the vulnerable Oracle WebLogic Server by sending a constructed HTTP GET request. Successfull exploitation manifests in the execution of malicious code under the security context of the user running WebLogic Server. The attacker will be able to compromise the weblogic server and gain access to the oracle database.	Artemis needs to validate the input of the data in the HTTP GET request in the URL. After the input is submitted, he URL cannot contain any data that shows the data. In other words, the vulnerable console class in Java can be triggered using a HTTP request.	4.6 Medium
Misconfigured AWS Storage	AWS data storage at Artemis is misconfigured. There are AWS security group misconfigurations and lack of access restrictions. Customers of AWS are responsible for security in the cloud such as applications, operating sytems,etc. S3 is primarily used for data storage. One important type of S3 access control is AWS Identity and Access Management (IAM). S3 bucket policies can also be set in the S3 environment without accessing IAM.	S3 AWS Security Groups	In an attempt to exploit the AWS data storage vulnerability, the pentester runs the risk of viewing sensitive data.	Upon successful exploitaton of this vulunerability, the attacker can view, change and delete sensitive data when there are AWS security group misconfigurations and lack of access restrictions. In addition, systems can be compromised and malicious code can be executed.	To address the security access controls and secruity group misconfiguratons, Artemis needs to do the following: 1. enable granular access controls for the S3 bucket in the S3 environment. The attributes that need to be set are effect (deny or allow), the entity allowed or denied access, the action (get,read,write,etc), the resource the action will act on, and the conditions that are valid. 2. block public access on the buckets. There are four additonal options to choose from when this is done 3. AWS encrypts data in transit using HTTPS/TLS 4. For encrytion at rest use AWS key management service for server side encryption and encrypt the client side with AWS encryption SDK 5. Security groups are similar to network access control lists but at the instance level instead of at the subnet level. The SG will allow/deny traffic such as http, ftp, ssh, rdp, etc. Data from or to the internet will go through the SG before or after it goes through the EC2 instaance. Since SGs by default deny all rules Artemis needs to allow the following ports: a. port 3389 for RDP b. port 23 for SSH c. ports 80 and 443 for the Web server d. port 1521 for the Oracle database e. ports 7001 and 8001 for the Oracle Weblogic Servers	7.2 High
Microsoft Exchange Server (CVE-2021-26855)	Microsoft Exchange Server is vulnerable to CVE-2021-26855. This is a zero-day vulnerability on Microsoft Exchange Servers which allows the attacker to send arbitrary HTTP requests and authenticate as the Exchange server. This is also know as server-side-request forgery (SSRF) vulnerability. SSRF is a web vulnerability that allows an attacker to prompt the server-side application to make HTTP requests to a random domain of the attacker's preference. In other words, the server fetches the URL requested by the attacker and sends the response back to the attacker. A SSRF attack utilizes an insecure server within the domain as a proxy.	Microsoft Exchange Server 2013 Microsoft Exchange Server 2016 Microsfot Exchange Server 2019	When the pentester attemps to exploit the vulnerability such as running a network scan, a network bottleneck might occur.	Upon successful exploitation of this vulnerability, the attacker can: 1. scan the entire network 2. retrieve sensitive information 3. use SSRF to escalate attacks further	Artemis needs to perform the following steps to remediate this vulnerability: 1. install all mandatory patches 2. place the Exchange server inside a VPN to separate port 443 from external connection requests 3. if the application needs to pass URLs in requests, whitelists for IP addresses and domains need to be used.	8.2 High