Scenario	Description of Vulnerability	Operating System/Versions Affected	Risks of Attemping to Exploit	Risk	Blocking Mechanisms	Remediation Action	CVSS Score
1	-Remote Desktop Protocol (RDP) is left unpatched and open to the Internet, giving attackers access to the server and possibly the corporate network.	-Windows 7, Windows 8, and Windows 10	-Trying to take advantage of the flaw can cause the host to crash or lock out an account.	-If an exploit were to be successful, an attacker may acquire access to the company network and possibly conduct attacks against internal systems, gather password hashes, crack passwords, gain access to other systems, move laterally, and other things.	-To stop an intrusion, blocking mechanisms like firewalls, antivirus software, and intrusion prevention systems (IPS) may be deployed.	-To prevent an attacker from exploiting the vulnerability, it should be patched as soon as possible.	7.5 (High)
2	-An attacker might access a web application'sback-end database through SQL injection and potentially edit or remove data.	-Any operating system that runs the vulnerable web application.	-A successful exploit attempt has the potential to bring down the host, lock out a user, or corrupt data in the back-end database.	-If a vulnerability is successfully exploited, a user could access other systems, change or remove data, or access the back-end database.	-To stop an attacker from taking advantage of the vulnerability, blocking techniques can be implemented, such as input validation, web application firewalls, or antivirus software.	-To prevent an attacker from exploiting the vulnerability, it should be patched as soon as possible.	8.8(High)
3	-The Cisco admin site contains a default password that hasn't been updated, which makes it possible for an attacker to access the router and potentially the corporate network.	-Cisco Routers.	-Exploiting the vulnerability can cause the host to crash or lock out an account.	-If an exploit were to be successful, an attacker may acquire access to the company network and possibly conduct attacks against internal systems, gather password hashes, decipher passwords, gain access to other systems, move laterally, and other things.	-To stop an attacker from abusing the system, blocking mechanisms like firewalls, intrusion prevention systems (IPS), or antivirus software may be deployed.	-To prevent an attacker from exploiting Vulnerabilities, default passwords should be changed as soon as possible.	8.8(High)
4	- The CVE-2019-0211 vulnerability affects the Apache web server, making it possible for an attacker toaccess the server and potentially the corporate network.	-Are versions of the Apache web server prior to 2.4.37.	-Exploiting the vulnerability can cause the host to crash or lock out an account.	-If an exploit were to be successful, an attacker may acquire access to the company network and possibly conduct attacks against internal systems, gather password hashes, decipher passwords, gain access to other systems, move laterally, and other things.	-To stop an attacker from exploiting the system Vulnerabilities, blocking mechanisms like firewalls, intrusion prevention systems (IPS), or antivirus software may be deployed.	-To prevent an attack from exploiting Vulnerabilities, they should be patched as soon as possible.	9.8(Critical)
5	-The web server is disclosing sensitive information that could be accessed by an attacker, including usernames, passwords, and credit card details.	-Any operating system that runs the vulnerable web server is impacted.	-Exploiting the vulnerability could possibly cause the host to crash or lock out an account.	-If an attack is successful, the attacker could acquire private information and possibly use it maliciously.	-An attacker can't take advantage of the vulnerability if blocking mechanisms like encryption, input validation, web application firewalls, or antivirus software are in place.	-Access to the data should be limited and should be encrypted as soon as possible to prevent an attacker from exploiting it.	5.3(medium)
6	-The online application has access control issues, making it vulnerable as a result, an attacker might potentially enter the business network or obtain access to sensitive data.	-Running the vulnerable web application on any operating system.	-Exploiting the vulnerability could bring down the host, lock out a user, or corrupt data in the back-end database.	-If successfully exploited, an attacker might access confidential information or the company network and possibly start an assault on internal systems, gather password hashes, crack passwords, get access to other systems, move laterally, and other things.	-Web application firewalls, input validation, antivirus software can be used to prevent an attacker from exploiting the vulnerability.	-To prevent an attacker from exploiting Vulnerabilities the acces control should be fixed as soon as possible.	7.5(high)
7	-Oracle WebLogic Server has a vulnerability identified as CVE-2020-14882 , which enables an attacker to access the server and perhaps the corporate network.	-Oracle WebLogic Server versions 10.3.6.0.0 and prior are affected.	-Exploiting the vulnerability can cause the host to crash or lock out an account.	-If an exploit were to be successful, an attacker may acquire access to the company network and possibly conduct attacks against internal systems, gather password hashes, decipher passwords, gain access to other systems, move laterally, and other things.	-To stop an attacker from taking advantage of the vulnerability, blocking methods like firewalls, intrusion prevention systems (IPS), or antivirus software may be utilized.	-To prevent an attacker from exploiting Vulnerabilities they should be patched as soon as possible.	9.8(Critical)
8	-As a misconfigured cloud storage system that could give an attacker access to confidential information or even the business network.	-Any cloud storage system that is misconfigured in a susceptible way.	-Exploiting the vulnerability can cause the host to crash or lock out an account.	-f successfully exploited, a hacker might access confidential information or the company network, where they could then potentially target internal systems, gather password hashes, crack passwords, gain access to other systems, move laterally, etc.	-Access control lists, encryption, or antivirus software are examples of blocking mechanisms to prevent an attacker from exploiting the vulnerability.	-To prevent an attacker from exploiting Vulnerabilities, misconfiguration should be fixed as soon as possible.	7.8 (High)
9	-The CVE-2021-26855 vulnerability in Microsoft Exchange Server makes it possible for an attacker to access the server and perhaps the corporate network.	-Versions of Microsoft Exchange Server 2013 through 2019.	-Exploiting the vulnerability can cause the host to crash or lock out an account.	-An attacker might theoretically attack internal systems, get password hashes, crack passwords, access other systems, move laterally, and more if they were able to successfully exploit the corporate network.	-Antivirus software, Intrusion Prevention Systems (IPS), or firewalls are examples of blocking methods that could be used to stop an attacker from taking advantage of the vulnerability.	-To prevent an attacker from exploiting a vulnerability, it should be patched as soon as possible.	9.8 (Critical)