Description of the vulnerability	Operating
Unpatched RDP is exposed to the internet	Microsoft Windows
Web application is vulnerable to SQL Injection	Linux, Windows, Unix, Mac
Default password on Cisco admin portal	Windows, Linux
Apache web server vulnerable to CVE-2019-0211	Linux, Mac
Web server is exposing sensitive data	Linux, Windows, Unix, Mac
Web application has broken access control	Linux, Windows, Unix, Mac
Oracle WebLogic Server vulnerable to CVE-2020-14882	Linux, Windows, Unix
Misconfigured cloud storage (AWS security group misconfiguration, lack of access restrictions)	Linux, Windows, Unix, Mac
Microsoft Exchange Server vulnerable to CVE-2021-26855	Windows

Risks of attempting to exploit

-A possible massive inflow of failed log in attempts which could cause storage issues with logs
-Network disruption

-Excess query attempts that may cause issues with the database
-Depending on the SQL injection, even if the attacker doesn't get the information they want; they could cause damage to the database

-Possible lock out of account

-Code not in favor of the attack could still damage the web server or connected endpoints

-None

-Possible lock out of account
-None.
-Very straightforward vulnerability that would not need many attempts or any other disruption method
-Possible to overwhelm the network while trying to figure out exactly what is misconfigured

-Possible network disruption

Risk (what could you or a threat actor do upon successful exploitation)?

-Gaining access to a user's workstation (possibly high level)
-Downloading and installing backdoors and malware to achieve persistence
-Breaching of all information accessible by the user (due to access control failures, possibly many if not all users)
-Gain a strong foothold to begin privilege escalation

-Unauthorized viewing of tables, views, and the entire database
-Deletion/alteration of entire tables/databases
-The attacker could gain administrative rights to a database which can open more footholds into the network.

-The attacker could gain full access to the portal to change, update, download copies, and delete anything they'd like
-The attacker could eavesdrop on the portal, siphoning data/information the entire time until they are spotted and

-Gain the ability to execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard
-Exposed data can be recorded by the attacker
-Failure with compliance
-Loss of clientele

-If an attacker gains access to a user's account (even low level), the attacker may be able to execute actions of a similar yet different level or worse, a higher level account than its own.

-Allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server.
-Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server
-If an attacker gains a foothold into the cloud, this vulnerability will make it much easier to escalate privilege and access information that is normally harder to reach
-Allow an attacker to remotely execute malicious code on a computer
-Code executed, could steal or alter information or alter the infrastructure with the server

Remediation action	CVSS score
-Verify compatibility with the needed patch and apply immediately	6-9
-White list inputs	
-Black list inputs	
-Input validation	
-Parametrized queries including prepared statements	
	5-7.5
-Update with strong password	
-Conduct thorough testing of the portal to confirm no persistence of an ongoing attack	10.00
-Review compatibility of attached services/processes and update the server to the latest stable version as soon as possible	
-Verify that the principle of least privilege is strict	7.20
-Secure the data with strong and up to date encryption and hashing suites	
-Clarify specifically why the data is being exposed and correct the issue	6-10
-Review the best practices for access control	
-Automate access control	
-Set alerts for access control	4-9
-Verify compatibility and update the server to the latest stable version as soon as possible	10.00
-Reconfigure and regularly test the configurations to make sure they work as intended	
-Ensure users/admins are up to date with aws certifications	4-9
-Update the server to the latest stable version as soon as possible	7.50