Description of the vulnerability	Operating systems/versions affected	Risks of attempting to exploit	Risk	Remediation action	CVSS score
Unpatched RDP is exposed to the internet	Windows/Linux	Time consuming /consistly changing IP address	If code is excuted properly attacker could inject BlueKeep /wormable exploit	configure firewall so no traffic can come though except traffic from allow-listed ip address ranges for authorized personnel / invest in more cloud services to remediate this issue from currenting the future	7.5
Web application is vulnerable to SQL Injection	Atremis web application /Redhat/Windows	being locked out by system /block by firewall /IP banned	loss of sensitve data,lost of application control ,delete data or destroy backups .disvastating loss to company applications	Use prepared statements with paramenterized queries/use of properly constructed stored procesures /allow-list input validation	9.8
Default password on Cisco admin portal	Cisco IOS	Host ban/IP banned /locked out /network outage	Loss of control of network/Traffic interference /Lost of sensitve data / loss of availabitty and confidentiality	adhere to password work policy/best pratices , standards and controls	8
Apache web server vulnerable to CVE-2019-0211	Linux/Red Hat /HTTP Server 2.4. 17 - 2.4.	None vulnerability found in apache	lost of customer data,PII,PHI,lost of availablity, confidential,Integrity, massive system breach /possbile DoD	Upgrade to the lastest Apache HTTP version	7.5
Web server is exposing sensitive data	Windows/RedHat	Blocked by IPS/IDS	Loss of data and confidentialty	Disable caching and autocomplete/store stronger passwords, proper data encryption/updated protocols apply access controls data classificaton	9.8
Web application has broken access control	Windows/LinuxRedHat	IPS/IDS interference /firewall block/NAC	Priviledge escalation/lose control of web app/availability loss	Routinely check access controls and consistently apply best pratices	8.8
Oracle WebLogic Server vulnerable to CVE-2020-14882	RedHat/Windows	detected by IPS/IDS	Take over of Oracle WebLogic Server impacts Confidentialty,Integrity and Availbility	Patch mangement /install new patch	9.7
Misconfigured cloud storage (AWS security group misconfiguration, lack of access restrictions)	Window/RedHatLinux	Loss of network functions/IPS/IDS Detection	Loss of Sensitive data ,Privilage escalation,impacts Confidentiality ,Integrity,Availbiltity	adhere to best pratices , automate policies on IAM/,audits regularly	9.5
Microsoft Exchange Server vulnerable to CVE-2021-26855	Windows	IPS/IDS Detection /blocked ip	Loss of data via email ,phone,text ,IM,partial impact to Confidentiality ,Integrity ,Avaibility	patch management /Mircosoft Defender automaticly mitigates CVE 2021-26855	8.6