Risk Number	Description of the Vulnerability	Systems Affected	Risk of Attempting to Exploit	Risk	Attack Vectors	Blocking Mechanisms	Remediation Action	Overall CVSS Score	Severity
1	**Unpatched RDP is exposed to the internet**	ALL Windows devices	- Malware injection - Data theft - Ransomware installation	- Unauthorized access to Windows devices - Undetected backdoors installed on Windows devices - Potential to move laterally within the network	- Brute forcing RDP credentials - Exploiting known RDP vulnerabilities	- Network-level firewalls - IDS or IPS - AD ACL	- Update all network devices with latest patches - Remove all old unsupported hardware - Disable RDP on all devices and configure Cisco, Fortinet, and Palo Alto network firewalls to block inbound/outbound RDP connections - Review list of staff members with remote access privileges and install up-to-date Zscaler on their systems - Provide sufficient training and resources for staff members with Zscaler access	8.1	High
2	**Web application is vulnerable to SQL injection**	ERP System (Oracle 12c)	- Modification/deletion of database records - Data leak - Exposure of sensitive database records	- Exfiltration of sensitive user data - Potential to gain administrative access to application - Execute arbitrary SQL queries	Manipulating input fields to inject malicious SQL queries	- Server-side input validation - Parameterized queries	- Enable server-side input validation (ERP database) - Disable client-side input validation (ERP database)	9.2	Critical
3	**Default password on Cisco admin portal**	Cisco devices	- Malicious configuration changes - Network disruption	- Gain administrative access to Cisco devices and modify critical network configurations - Staging for MITM attacks - Launch network-level attacks	- Log in using default credentials - Brute-force known default passwords	- Change default password at set-up - Enable MFA	- Change default passwords for all Cisco devices - Follow strong password practices (such as use of long passphrase and mixed punctation) - Enable MFA for Cisco devices OR - Finish phasing out Cisco devices as planned, and apply above remediation to Fortinet Fortigate devices	8	High
4	**Apache web server vulnerable to CVE-2019-0211**	Apache web servers (on-prem servers)	- Privilege escalation - Unauthorized access to sensitive files - Potential compromise of on-prem servers and lateral movement in network	- Gain root access - Install malware/backdoors - Access and tamper with critical server files	Exploit vulnerability to run scripts and gain root access	- Apply security updates	- Apply latest updates for Apache web server - Apply latest patches for web server system's OS	7.8	High
5	**Web server is exposing sensitive data**	AWS Servers	- Unauthorized access to sensitive server data - Data leak/breach - Violation of privacy regulations	- Extraction of sensitive data, such as PID, passwords, or financial details - Use of exposed data for identity theft	- Directly accessing exposed files/directories - Directory traversal - Use Google Dorks to find exposed content	- Well-implemented file and directory permissions - Routine vulnerability assessments prior to moving code to production	- Review and adjust file and directory permissions for AWS servers - Perform security audit and comprehensive vulnerability scans to identify exposure points - Review security checks/security scripts in development cycle effectiveness	7.2	High
6	**Web application has broken access control**	PARS, APOLLO	- Breach of user privacy - Unauthorized manipulation of application code and functionality	- Access restricted features - Modify/delete critical data - Impersonation of other users	- Session hijacking - Lack of authentication/authorization enforcement	- Properly configured access control following least privilege - Network segmentation - Multifactor Authentication	- Review Microsoft AD configuration and establish RBAC, following least privilege principle - Enable MFA on top of already-existing SSO	7.8	High
7	**Oracle WebLogic Server vulnerable to CVE-2020-14882**	ERP System (Oracle 12c)	- Remote code execution - Compromise of affected server - Data theft/manipulation	- Execute arbitrary commands on server - Installation of malicious software	Exploit CVE-2020-14882 vulnerability using crafted HTTP requests	- Apply security updates	- Apply latest updates for Oracle12c database (ERP system) - Apply latest patches for Linux OS (ERP system)	9.8	Critical
8	**Misconfigured cloud storage (AWS security group misconfiguration, lack of access restrictions)**	AWS Servers, AWS Cloud Storage, Office 365 applications using cloud storage	- Unauthorized access to sensitive data stored in cloud - Data leak/breach - Violation of privacy regulations	- Access to sensitive cloud data - Modify/delete cloud data	- Directly accessing exposed cloud storage and s3 buckets - Use Google Dorks to find exposed buckets	- Well-configured access controls	- Review and update access controls, permissions, and configurations on AWS servers, AWS cloud storage, and Office 365 applications	7.5	High
9	**Microsoft Exchange Server vulnerable to CVE-2021-26855**	Office 365 Messaging, On-prem Microsoft Exchange Servers	- Remote code execution - Unauthorized access to emails and sensitive info - Data manipulation	- Execute arbitrary code on server - Access user emails and attachments - Access confidential proprietary information	Exploit CVE-2021-26855 using crafted HTTPS requests	- Apply Microsoft patches - VPN	- Apply Microsoft security patches AND move Exchange servers to inside of VPN, to reject HTTPS requests	9.1	Critical