Description	Operating Systems/Versions	Risks of attempting to exploit	Risk	Remediation action	CVSS score	Risk Owner	Key Control
In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter)	This impacts all Apache HTTP Server releases from 2.4.17 to 2.4.38.	An attacker could execute arbitrary code with root privilages to manuplate the scoreboard	in this scenario, users with limited permissions could exploit the flaw to get root privileges using scripts and run commands on vulnerable Apache web servers.	Upgrading to version 2.4.39	7.8	Risk services	Yes
Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware	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.	Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server.	An attacker can take control over the server.	Installing patches	9.8	Risk services	Yes
CVE-2021-26855 is a vulnerability on Microsoft Exchange Server that allows an attacker bypassing the authentication and impersonating as the admin.	Microsoft Exhcange Server 1013, 2016, and 2019	Remote attacker could exploit this flaw by sending a specially crafted HTTP request to a vulnerable Exchange Server.	When exploited, HTTPS connections are established to authenticate user access.	Microsoft released out-of-band patches for Microsoft Exchange Server on March 2	9.1	Risk services	Yes
a SQL injection is when criminal hackers enter malicious commands into web forms, like the search field, login field, or URL, of an unsecure website to gain unauthorized access to sensitive and valuable data.	Any procedure that constructs SQL statements	A successful attack could allow any data in the remote MySQL database to be read or modified	A vulnerability in the MySQL Server database could allow a remote, authenticated user to inject SQL code that runs with high privileges on a remote MySQL Server database.	Use regular expressions as whitelists for structured data (such as name, age, income, survey response, zip code) to ensure strong input validation.	6.5	Risk services	Yes
Unpatched RDP is exposed to the internet	All windows versions.	An attacker who successfully exploited this vulnerability could obtain information to further compromise the user's system.	An attacker is given read access to the server process	If you no longer need these services on your system, consider disabling them as a security best practice. Disabling unused and unneeded services helps reduce your exposure to security vulnerabilities.	7.5	Risk services	Yes
Defualt login being used on cisco devices	Cisco devices	A vulnerability in Cisco Ultra Services Framework Element Manager could allow an authenticated, remote attacker with access to the management network to log in to the affected device using default credentials present on the system.	An exploit could allow an attacker with access to the management network to log in to the affected device using default credentials present on the system.	Use a more secure password.	6.3	Risk services	Yes
A web application running on the remote host uses a Java framework that is affected by a broken access control vulnerability.	All known web servers, application servers, and web application in the network.	An attacker can gain access to sensitive information	The attacker can exploit the vulnerability to gain control	Upgrade to the latest patch to make sure the web application is secure.	5.8	Risk services	No
Web server exposing sensitive data	ALl web servers	As a result a malicious user can extract sensitive data from the web server and in some cases use this vulnerability in order to get a remote code execution on the remote web server.	An attacker can easily extract sensitive data from the server	Encrypt data, prevent password attacks, secure authenication gateways	9.8	Risk services	Yes