Proposed Vulnerabilities	SNYK		Trivy		OWASP DC	
	CVE Numbers	Description	CVE Numbers	Description	CVE Numbers	Description
V1: Exposed API Endpoints without Authentication.					CVE-2021-3807	improper access control identified in 2021
V2: Accidental Exposure of Sensitive API Endpoints.						
V3: Unknown/ Untrusted APIs.						
V4: Weak authentication mechanisms for APIs.					CVE-2020-28168	improper access control identified in 2020
V5: Insecure data serialization.					CVE-2021-23343	unauthorized access identified in 2021
V6: Misconfiguration of API gateways.					CVE-2020-7598	improper access control identified in 2020
V7: Service Registration Poisoning.						
V8: Unauthorized Access to Service Discovery.						
V9: Unavailability of Service Registration Validation.	CVE-2021-28918	injection vulnerability identified in 2021				
	CVE-2021-29418	data leak vulnerability identified in 2021				
	CVE-2023-3341	information disclosure identified in 2023				
V10: Unauthorized Service Deregistration.						
V11: Reuse of Previous Service Requests.						
V12: Legitimate Service Spoofing.						
V13: Insufficient Network Segmentation.						
V14: Improper Service Mesh Implementation.						
V15: Misconfigured Network Access Controls.						
V16: Incorrect Firewall Configuration.						
V17: No Internet Traffic Encryption.						
V18: Using Default Network Configurations.						
V19: Using Weak or Deprecated Algorithms.						
V20: Lack of End-to-End Encryption.						
V21: Sensitive Data Exposure via Metadata.						
V22: Improper Encryption Key Management.						
V23: Improper Validation of Certificates.						
V24: Hardcoded Encryption Keys.						
V25: No Proper Rate Limiting.	CVE-2019-1559	improper access control identified in 2019				
	CVE-2021-3778	denial of service identified in 2021				
	CVE-2021-46143	denial of service identified in 2021				
V26: Improper Handling of Suspicious.	CVE-2014-2583	denial of service identified in 2014				
	CVE-2014-9114	denial of service identified in 2014				
	CVE-2020-24977	denial of service identified in 2020				
	CVE-2022-23990	denial of service identified in 2022				
	CVE-2016-4487	denial of service identified in 2016				
	CVE-2022-2817	denial of service identified in 2022				
V27: Lack of Individualized Rate Limiting.	CVE-2015-0247	denial of service identified in 2015			CVE-2022-0155	denial of service identified in 2022
	CVE-2022-22822	denial of service identified in 2022				
	CVE-2020-27618	denial of service identified in 2020				
	CVE-2020-35493	denial of service identified in 2020				
	CVE-2021-33574	denial of service identified in 2021				
	CVE-2022-3153	denial of service identified in 2022				
	CVE-2022-3219	denial of service identified in 2022				
	CVE-2022-47008	denial of service identified in 2022				
	CVE-2023-0049	denial of service identified in 2023				
V28: Improper Configuration of Rate Limits.	CVE-2018-1000876	denial of service identified in 2018			CVE-2022-25883	denial of service identified in 2022
	CVE-2019-18348	denial of service identified in 2019				
	CVE-2020-8492	denial of service identified in 2020				
	CVE-2021-3517	denial of service identified in 2021				
	CVE-2021-37322	denial of service identified in 2021				
	CVE-2022-23308	denial of service identified in 2022				

	CVE-2010-4756	denial of service identified in 2010				
	CVE-2017-5969	denial of service identified in 2017				
	CVE-2020-19187	denial of service identified in 2020				
	CVE-2021-28153	denial of service identified in 2021				
	CVE-2022-2182	denial of service identified in 2022				
	CVE-2022-2344	denial of service identified in 2022				
V29: Targeted API Abuse.	CVE-2020-27619	denial of service identified in 2020			CVE-2020-26274	denial of service identified in 2020
	CVE-2022-1629	denial of service identified in 2022				
	CVE-2020-19724	denial of service identified in 2020				
	CVE-2022-2946	denial of service identified in 2022				
	CVE-2023-0433	denial of service identified in 2023				
	CVE-2023-0464	denial of service identified in 2023				
V30: Weak or Non-existent Database Encryption.	CVE-2022-1271	information disclosure identified in 2022	CVE-2022-25881	data leak vulnerability identified in 2022		
	CVE-2017-0663	information disclosure identified in 2017				
	CVE-2018-1122	information disclosure identified in 2018				
	CVE-2019-17498	information disclosure identified in 2019				
	CVE-2021-45960	information disclosure identified in 2021				
	CVE-2022-43551	data leak vulnerability identified in 2022				
	CVE-2018-14618	data leak vulnerability identified in 2018				
	CVE-2022-2571	information disclosure identified in 2022				
	CVE-2022-2580	information disclosure identified in 2022				
V31: Inadequate Database Hardening.	CVE-2018-20843	data leak vulnerability identified in 2018	CVE-2022-24999	data leak vulnerability identified in 2022		
	CVE-2021-3541	denial of service identified in 2021	CVE-2019-18276	information disclosure identified in 2019		
	CVE-2021-35942	denial of service identified in 2021				
	CVE-2023-5388	information disclosure identified in 2023				
	CVE-2016-4489	information disclosure identified in 2016				
	CVE-2018-16428	information disclosure identified in 2018				
	CVE-2018-20482	data leak vulnerability identified in 2018				
	CVE-2020-35495	information disclosure identified in 2020				
	CVE-2022-2207	data leak vulnerability identified in 2022				
V32: Using Default Database Credentials.	CVE-2020-7778	unauthorized access identified in 2020	CVE-2018-5407	information disclosure identified in 2018	CVE-2021-33502	data leak vulnerability identified in 2021
	CVE-2021-23406	information disclosure identified in 2021			CVE-2020-26245	information disclosure identified in 2020
	CVE-2009-5155	information disclosure identified in 2009				
	CVE-2017-16931	data leak vulnerability identified in 2017				
	CVE-2017-7375	data leak vulnerability identified in 2017				
	CVE-2018-12384	data leak vulnerability identified in 2018				
	CVE-2020-19726	data leak vulnerability identified in 2020				
	CVE-2021-3518	data leak vulnerability identified in 2021				
	CVE-2021-3999	data leak vulnerability identified in 2021				
	CVE-2016-3120	data leak vulnerability identified in 2016				
	CVE-2019-12972	information disclosure identified in 2019				
	CVE-2020-35494	data leak vulnerability identified in 2020				
	CVE-2022-2126	data leak vulnerability identified in 2022				
	CVE-2022-2862	information disclosure identified in 2022				
	CVE-2022-3234	data leak vulnerability identified in 2022				
	CVE-2022-3591	information disclosure identified in 2022				
	CVE-2023-2609	information disclosure identified in 2023				
	CVE-2023-45322	information disclosure identified in 2023				
V33: Exposure of Sensitive Data via Error Messages.	CVE-2016-2781	information disclosure identified in 2016				
	CVE-2016-9427	data leak vulnerability identified in 2016				
V34: Non-existent Data Integrity Checks.	CVE-2016-2183	buffer overflow identified in 2016			CVE-2023-43646	data leak vulnerability identified in 2023
	CVE-2019-19603	data leak vulnerability identified in 2019				

	CVE-2019-5188	information disclosure identified in 2019				
	CVE-2020-25709	data leak vulnerability identified in 2020				
	CVE-2021-3516	information disclosure identified in 2021				
	CVE-2021-38185	data leak vulnerability identified in 2021				
	CVE-2017-1000382	data leak vulnerability identified in 2017				
	CVE-2017-14939	data leak vulnerability identified in 2017				
	CVE-2019-17023	data leak vulnerability identified in 2019				
	CVE-2022-38533	data leak vulnerability identified in 2022				
V35: SQL Injection.	CVE-2018-5407	information disclosure identified in 2018			CVE-2023-45857	remote code execution identified in 2023
	CVE-2020-8622	remote code execution identified in 2020				
	CVE-2021-23343	unauthorized access identified in 2021				
	CVE-2021-3796	remote code execution identified in 2021				
	CVE-2022-3715	remote code execution identified in 2022				
	CVE-2022-37434	remote code execution identified in 2022				
	CVE-2019-17450	remote code execution identified in 2019				
	CVE-2019-18276	information disclosure identified in 2019				
	CVE-2020-21490	remote code execution identified in 2020				
	CVE-2022-2819	remote code execution identified in 2022				
	CVE-2022-3037	remote code execution identified in 2022				
	CVE-2022-3520	remote code execution identified in 2022				
	CVE-2022-35205	remote code execution identified in 2022				
	CVE-2022-47007	remote code execution identified in 2022				
	CVE-2022-47696	remote code execution identified in 2022				
	CVE-2023-2610	remote code execution identified in 2023				
V36: Cross-Site Scripting (XSS).	CVE-2022-25313	cross-site scripting (XSS) identified in 2022			CVE-2021-44906	cross-site scripting (XSS) identified in 2021
					CVE-2021-21388	cross-site scripting (XSS) identified in 2021
V37: Command Injection.	CVE-2019-3855	privilege escalation identified in 2019	CVE-2019-11745	buffer overflow identified in 2019	CVE-2020-28500	buffer overflow identified in 2020
	CVE-2018-14404	buffer overflow identified in 2018	CVE-2016-2183	buffer overflow identified in 2016		
	CVE-2020-12243	buffer overflow identified in 2020	CVE-2018-1000001	buffer overflow identified in 2018		
	CVE-2020-36228	buffer overflow identified in 2020				
	CVE-2021-25220	buffer overflow identified in 2021				
	CVE-2021-3712	buffer overflow identified in 2021				
	CVE-2021-3872	buffer overflow identified in 2021				
	CVE-2022-23218	buffer overflow identified in 2022				
	CVE-2022-40304	buffer overflow identified in 2022				
	CVE-2022-42012	buffer overflow identified in 2022				
	CVE-2015-1572	buffer overflow identified in 2015				
	CVE-2018-16429	buffer overflow identified in 2018				
	CVE-2019-15903	buffer overflow identified in 2019				
	CVE-2019-5436	buffer overflow identified in 2019				
	CVE-2019-9674	buffer overflow identified in 2019				
	CVE-2022-0536	privilege escalation identified in 2022				
	CVE-2022-2210	buffer overflow identified in 2022				
	CVE-2022-47695	buffer overflow identified in 2022				
	CVE-2023-0465	buffer overflow identified in 2023				
V38: Insecure Deserialization of Data.						
V39: User Inputs Directly Accessing Objects.	CVE-2019-11745	buffer overflow identified in 2019	CVE-2021-33502	data leak vulnerability identified in 2021	CVE-2022-33987	buffer overflow identified in 2022
	CVE-2019-16056	buffer overflow identified in 2019			CVE-2022-31129	buffer overflow identified in 2022
	CVE-2019-20454	buffer overflow identified in 2019			CVE-2023-26115	buffer overflow identified in 2023
	CVE-2019-9924	buffer overflow identified in 2019				
	CVE-2020-13630	buffer overflow identified in 2020				
	CVE-2022-48565	buffer overflow identified in 2022				

	CVE-2022-48063	buffer overflow identified in 2022				
V40: Granting Higher than Required Level of Access.						
V41: Credential Hardcoding in Source Code.						
V42: Granted Privilege Exploitation.						
V43: Race Condition Exploitation.					CVE-2020-7774	data leak vulnerability identified in 2020
V44: Improper Data Transaction Management.					CVE-2022-24999	data leak vulnerability identified in 2022
					CVE-2020-7752	data leak vulnerability identified in 2020
V45: Insecure Data Synchronization.	CVE-2019-13050	data leak vulnerability identified in 2019			CVE-2022-25881	data leak vulnerability identified in 2022
	CVE-2020-36224	information disclosure identified in 2020			CVE-2020-7751	information disclosure identified in 2020
	CVE-2022-40303	data leak vulnerability identified in 2022				
	CVE-2023-36632	information disclosure identified in 2023				
	CVE-2023-37920	information disclosure identified in 2023				
	CVE-2019-1010023	information disclosure identified in 2019				
V46: Concurrent Data Access Mismanagement.	CVE-2022-27782	information disclosure identified in 2022	CVE-2018-12384	data leak vulnerability identified in 2018		
	CVE-2020-16598	data leak vulnerability identified in 2020				
	CVE-2022-1720	data leak vulnerability identified in 2022				
	CVE-2023-0512	data leak vulnerability identified in 2023				
V47: Lack of Regular Backups.	CVE-2022-22826	data leak vulnerability identified in 2022				
	CVE-2021-3903	data leak vulnerability identified in 2021				
	CVE-2021-3927	data leak vulnerability identified in 2021				
	CVE-2022-47673	information disclosure identified in 2022				
V48: Insecure Backup Storage.	CVE-2020-7774	data leak vulnerability identified in 2020	CVE-2018-5743	data leak vulnerability identified in 2018		
	CVE-2020-8617	data leak vulnerability identified in 2020				
	CVE-2017-11368	data leak vulnerability identified in 2017				
	CVE-2022-22823	information disclosure identified in 2022				
	CVE-2020-16599	information disclosure identified in 2020				
	CVE-2022-2923	data leak vulnerability identified in 2022				
	CVE-2022-48065	information disclosure identified in 2022				
V49: Lack of Backup Validation.	CVE-2020-8616	injection vulnerability identified in 2020	CVE-2019-12749	data leak vulnerability identified in 2019		
	CVE-2019-13057	data leak vulnerability identified in 2019				
	CVE-2020-36225	information disclosure identified in 2020				
	CVE-2019-19244	data leak vulnerability identified in 2019				
V50: Improper Disposal of Outdated Backups.	CVE-2023-4421	information disclosure identified in 2023				
V51: Insecure/Weak Authentication.	CVE-2019-9740	unauthorized access identified in 2019				
	CVE-2023-45853	unauthorized access identified in 2023				
	CVE-2022-2129	improper access control identified in 2022				
V52: Enumeration of Accounts.	CVE-2020-8203	privilege escalation identified in 2020				
	CVE-2021-43138	injection vulnerability identified in 2021				
	CVE-2019-13565	improper access control identified in 2019				
	CVE-2021-44906	cross-site scripting (XSS) identified in 2021				
V53: Continued Usage of Breached Credentials.	CVE-2019-17007	remote code execution identified in 2019				
	CVE-2022-27781	unauthorized access identified in 2022				
	CVE-2022-48064	improper access control identified in 2022				
V54: Identity Federation Misconfiguration.	CVE-2021-23337	remote code execution identified in 2021				
	CVE-2019-13115	improper access control identified in 2019				
	CVE-2020-36221	improper access control identified in 2020				
	CVE-2015-1782	improper access control identified in 2015				
	CVE-2022-2125	unauthorized access identified in 2022				
	CVE-2022-2287	improper access control identified in 2022				
	CVE-2022-2343	improper access control identified in 2022				
	CVE-2022-2581	unauthorized access identified in 2022				
	CVE-2022-2874	improper access control identified in 2022				

	CVE-2023-2953	improper access control identified in 2023				
	CVE-2023-32611	improper access control identified in 2023				
V55: Provision of Higher Privileges.						
V56: Improper Token Invalidation.	CVE-2019-11729	unauthorized access identified in 2019	CVE-2019-1559	improper access control identified in 2019		
	CVE-2019-20907	unauthorized access identified in 2019				
	CVE-2020-36229	improper access control identified in 2020				
	CVE-2016-4490	unauthorized access identified in 2016				
	CVE-2017-6891	improper access control identified in 2017				
	CVE-2017-8872	improper access control identified in 2017				
	CVE-2022-0351	unauthorized access identified in 2022				
	CVE-2022-2816	unauthorized access identified in 2022				
	CVE-2022-3256	unauthorized access identified in 2022				
	CVE-2022-3296	unauthorized access identified in 2022				
V57: Insecure Access Token Storage.	CVE-2022-1619	unauthorized access identified in 2022				
V58: Embedded Static Credentials.	CVE-2022-2124	improper access control identified in 2022	CVE-2022-33987	buffer overflow identified in 2022		
V59: Reuse of Passwords.	CVE-2019-9169	improper access control identified in 2019				
V60: Vulnerable Password Recovery Process.	CVE-2017-15412	unauthorized access identified in 2017				
	CVE-2018-1061	unauthorized access identified in 2018				
	CVE-2021-3737	improper access control identified in 2021				
V61: MFA not Used/Enforced.	CVE-2021-3749	unauthorized access identified in 2021				
	CVE-2018-11236	improper access control identified in 2018				
	CVE-2023-23916	improper access control identified in 2023				
	CVE-2023-39615	improper access control identified in 2023				
	CVE-2021-3236	unauthorized access identified in 2021				
	CVE-2022-2345	unauthorized access identified in 2022				
V62: Phishing Attacks on Users.	CVE-2017-9050	improper access control identified in 2017			CVE-2021-21315	improper access control identified in 2021
	CVE-2020-25692	unauthorized access identified in 2020				
	CVE-2022-3517	improper access control identified in 2022				
	CVE-2017-17087	unauthorized access identified in 2017				
	CVE-2022-2598	improper access control identified in 2022				
V63: Unenforced Access Controls.	CVE-2017-9287	unauthorized access identified in 2017				
	CVE-2020-29573	unauthorized access identified in 2020				
	CVE-2022-42011	unauthorized access identified in 2022				
	CVE-2018-12934	unauthorized access identified in 2018				
	CVE-2022-35206	unauthorized access identified in 2022				
V64: Human Error in Granting Access.	CVE-2019-9948	improper access control identified in 2019				
	CVE-2020-28469	unauthorized access identified in 2020				
	CVE-2020-28500	buffer overflow identified in 2020				
	CVE-2022-2068	improper access control identified in 2022				
	CVE-2020-16593	improper access control identified in 2020				
V65: Insecure Direct Object Reference.	CVE-2018-5743	data leak vulnerability identified in 2018	CVE-2019-12735	remote code execution identified in 2019		
	CVE-2022-24999	data leak vulnerability identified in 2022				
	CVE-2017-7500	remote code execution identified in 2017				
	CVE-2020-26116	remote code execution identified in 2020				
	CVE-2021-4192	remote code execution identified in 2021				
	CVE-2023-29491	remote code execution identified in 2023				
	CVE-2016-4488	remote code execution identified in 2016				
	CVE-2016-4492	remote code execution identified in 2016				
	CVE-2020-12413	remote code execution identified in 2020				
	CVE-2022-48554	remote code execution identified in 2022				
V66: Vulnerable APIs Having Higher Control.	CVE-2019-9947	improper access control identified in 2019			CVE-2021-3749	unauthorized access identified in 2021
	CVE-2022-27778	improper access control identified in 2022				

	CVE-2016-4493	improper access control identified in 2016				
	CVE-2022-1154	improper access control identified in 2022				
	CVE-2022-47011	improper access control identified in 2022				
V67: Session Hijacking.	CVE-2005-2541	improper access control identified in 2005			CVE-2020-28469	unauthorized access identified in 2020
	CVE-2020-25648	improper access control identified in 2020				
	CVE-2021-20271	unauthorized access identified in 2021				
	CVE-2021-45078	improper access control identified in 2021				
	CVE-2022-0155	denial of service identified in 2022				
	CVE-2015-8865	unauthorized access identified in 2015				
	CVE-2016-6170	improper access control identified in 2016				
	CVE-2020-35496	improper access control identified in 2020				
	CVE-2022-2175	unauthorized access identified in 2022				
	CVE-2022-27943	improper access control identified in 2022				
	CVE-2022-3358	improper access control identified in 2022				
	CVE-2023-3817	improper access control identified in 2023				
	CVE-2023-46246	unauthorized access identified in 2023				
V68: Cross-Site Request Forgery.	CVE-2019-9636	improper access control identified in 2019			CVE-2020-7778	unauthorized access identified in 2020
	CVE-2019-19906	unauthorized access identified in 2019				
	CVE-2021-3326	unauthorized access identified in 2021				
	CVE-2020-35507	unauthorized access identified in 2020				
	CVE-2021-4166	unauthorized access identified in 2021				
	CVE-2021-43618	unauthorized access identified in 2021				
	CVE-2022-45703	improper access control identified in 2022				
V69: Session Control Exploitation.	CVE-2020-7752	data leak vulnerability identified in 2020	CVE-2019-9636	improper access control identified in 2019		
	CVE-2021-32640	privilege escalation identified in 2021				
	CVE-2022-1292	improper access control identified in 2022				
	CVE-2018-10360	unauthorized access identified in 2018				
V70: Improper Session Expiry.	CVE-2019-12735	remote code execution identified in 2019				
	CVE-2017-16997	improper access control identified in 2017				
	CVE-2020-22218	improper access control identified in 2020				
	CVE-2022-29824	improper access control identified in 2022				
	CVE-2022-2284	improper access control identified in 2022				
	CVE-2022-2285	improper access control identified in 2022				
	CVE-2023-0051	unauthorized access identified in 2023				
V71: Container Misconfigurations.	CVE-2021-33502	data leak vulnerability identified in 2021				
	CVE-2019-19956	privilege escalation identified in 2019				
	CVE-2021-27212	privilege escalation identified in 2021				
	CVE-2021-4019	privilege escalation identified in 2021				
	CVE-2016-9063	privilege escalation identified in 2016				
	CVE-2019-9070	privilege escalation identified in 2019				
V72: Improper Container Isolation.	CVE-2019-3857	cross-site scripting (XSS) identified in 2019				
	CVE-2019-19880	privilege escalation identified in 2019				
	CVE-2022-23219	privilege escalation identified in 2022				
	CVE-2022-25881	data leak vulnerability identified in 2022				
	CVE-2021-3826	privilege escalation identified in 2021				
	CVE-2022-44840	privilege escalation identified in 2022				
V73: Direct Storage of Sensitive Data on Container Image.	CVE-2021-21315	improper access control identified in 2021				
	CVE-2016-5131	remote code execution identified in 2016				
	CVE-2016-9318	remote code execution identified in 2016				
	CVE-2019-5827	remote code execution identified in 2019				
	CVE-2019-8457	remote code execution identified in 2019				
	CVE-2023-0215	remote code execution identified in 2023				

	CVE-2023-1579	remote code execution identified in 2023				
	CVE-2020-19185	remote code execution identified in 2020				
	CVE-2022-47010	remote code execution identified in 2022				
V74: Outdated/Insecure Container Image Usage.	CVE-2023-45857	remote code execution identified in 2023	CVE-2019-3855	privilege escalation identified in 2019		
	CVE-2019-20218	privilege escalation identified in 2019				
	CVE-2017-3735	privilege escalation identified in 2017				
V75: Misconfiguration of Orchestration Dashboards.	CVE-2020-26245	information disclosure identified in 2020			CVE-2022-0536	privilege escalation identified in 2022
	CVE-2018-0739	privilege escalation identified in 2018			CVE-2020-8203	privilege escalation identified in 2020
	CVE-2019-14866	privilege escalation identified in 2019				
	CVE-2021-39537	privilege escalation identified in 2021				
V76: Orchestration Tools Having Unrestricted API Access.						
V77: Poor Definition of RBAC.						
V78: Vulnerabilities in Orchestration Tools.	CVE-2017-1000158	privilege escalation identified in 2017				
	CVE-2019-3862	privilege escalation identified in 2019				
	CVE-2020-25710	privilege escalation identified in 2020				
	CVE-2020-7595	privilege escalation identified in 2020				
	CVE-2022-22825	privilege escalation identified in 2022				
	CVE-2016-3075	privilege escalation identified in 2016				
	CVE-2022-3352	privilege escalation identified in 2022				
V79: Insecure Service Configuration.						
V80: Service Deployments with no Configuration Validation.						
V81: Embedded Passwords/Tokens in Configuration Files.						
V82: Insecure Configuration File Validation.	CVE-2020-26274	denial of service identified in 2020	CVE-2019-17007	remote code execution identified in 2019		
	CVE-2017-7501	remote code execution identified in 2017				
	CVE-2020-28168	improper access control identified in 2020				
	CVE-2022-22824	remote code execution identified in 2022				
	CVE-2023-1127	remote code execution identified in 2023				
	CVE-2023-1264	remote code execution identified in 2023				
V83: Adding Components with Known Vulnerabilities.	CVE-2022-31129	buffer overflow identified in 2022			CVE-2021-23337	remote code execution identified in 2021
	CVE-2022-45061	remote code execution identified in 2022				
	CVE-2020-1968	remote code execution identified in 2020				
	CVE-2023-0466	remote code execution identified in 2023				
V84: Outdated/Unmaintained Dependency Usage.	CVE-2022-25883	denial of service identified in 2022	CVE-2020-8622	remote code execution identified in 2020		
	CVE-2022-43680	remote code execution identified in 2022				
	CVE-2020-19188	remote code execution identified in 2020				
V85: Insufficient Scanning of Dependencies.						
V86: No Transitive Dependency Validation.						
V87: Inconsistent Security Practices.						
V88: Issues Within Specific Libraries.						
V89: Misconfiguration of Different Platforms.						
V90: Patch Management Complexity.						
V91: Legacy System Integration Vulnerabilities.						
V92: Mismatched Data Formats in Different Technologies.						
V93: Service Mesh Configuration Errors.						
V94: Inconsistent Security at Integration Points.						
V95: Compromised Supply Chain Attacks.						
V96: Third-Party Components Service Outages.						
V97: Insecure Third-Party Components.						
V98: No Proper Security Practices in Third-Party Components.						
V99: Various Injection Vulnerabilities.	CVE-2019-12749	data leak vulnerability identified in 2019	CVE-2020-8616	injection vulnerability identified in 2020	CVE-2021-43138	injection vulnerability identified in 2021
	CVE-2019-3856	injection vulnerability identified in 2019	CVE-2019-3863	injection vulnerability identified in 2019	CVE-2022-24785	injection vulnerability identified in 2022
	CVE-2019-3863	injection vulnerability identified in 2019			CVE-2021-28918	injection vulnerability identified in 2021

	CVE-2017-16932	injection vulnerability identified in 2017				
	CVE-2018-1000007	injection vulnerability identified in 2018				
	CVE-2018-18508	injection vulnerability identified in 2018				
	CVE-2019-12450	injection vulnerability identified in 2019				
	CVE-2020-10735	injection vulnerability identified in 2020				
	CVE-2020-12403	injection vulnerability identified in 2020				
	CVE-2020-35342	injection vulnerability identified in 2020				
	CVE-2020-35527	injection vulnerability identified in 2020				
	CVE-2020-36226	injection vulnerability identified in 2020				
	CVE-2021-27218	injection vulnerability identified in 2021				
	CVE-2021-33560	injection vulnerability identified in 2021				
	CVE-2021-3984	injection vulnerability identified in 2021				
	CVE-2022-0359	injection vulnerability identified in 2022				
	CVE-2022-1621	injection vulnerability identified in 2022				
	CVE-2022-29155	injection vulnerability identified in 2022				
	CVE-2022-33987	buffer overflow identified in 2022				
	CVE-2023-2603	injection vulnerability identified in 2023				
	CVE-2023-2650	injection vulnerability identified in 2023				
	CVE-2014-3564	injection vulnerability identified in 2014				
	CVE-2016-9586	injection vulnerability identified in 2016				
	CVE-2018-6323	injection vulnerability identified in 2018				
	CVE-2020-19189	injection vulnerability identified in 2020				
	CVE-2020-19190	injection vulnerability identified in 2020				
	CVE-2020-35512	injection vulnerability identified in 2020				
	CVE-2020-35525	injection vulnerability identified in 2020				
	CVE-2022-2889	injection vulnerability identified in 2022				
	CVE-2022-2980	injection vulnerability identified in 2022				
	CVE-2023-27538	injection vulnerability identified in 2023				
	CVE-2023-5441	injection vulnerability identified in 2023				
V100: Improper XSS Prevention Implementation.	CVE-2014-3566	cross-site scripting (XSS) identified in 2014	CVE-2019-3857	cross-site scripting (XSS) identified in 2019		
	CVE-2021-3807	improper access control identified in 2021				
	CVE-2022-24785	injection vulnerability identified in 2022				
	CVE-2019-11756	cross-site scripting (XSS) identified in 2019				
	CVE-2019-17006	cross-site scripting (XSS) identified in 2019				
	CVE-2020-36223	cross-site scripting (XSS) identified in 2020				
	CVE-2020-36227	cross-site scripting (XSS) identified in 2020				
	CVE-2020-36632	cross-site scripting (XSS) identified in 2020				
	CVE-2020-8285	cross-site scripting (XSS) identified in 2020				
	CVE-2021-20294	cross-site scripting (XSS) identified in 2021				
	CVE-2021-21388	cross-site scripting (XSS) identified in 2021				
	CVE-2021-3487	cross-site scripting (XSS) identified in 2021				
	CVE-2021-3537	cross-site scripting (XSS) identified in 2021				
	CVE-2021-3733	cross-site scripting (XSS) identified in 2021				
	CVE-2022-22827	cross-site scripting (XSS) identified in 2022				
	CVE-2022-23852	cross-site scripting (XSS) identified in 2022				
	CVE-2022-27780	cross-site scripting (XSS) identified in 2022				
	CVE-2022-3094	cross-site scripting (XSS) identified in 2022				
	CVE-2022-42010	cross-site scripting (XSS) identified in 2022				
	CVE-2010-1634	cross-site scripting (XSS) identified in 2010				
	CVE-2012-5644	cross-site scripting (XSS) identified in 2012				
	CVE-2015-8777	cross-site scripting (XSS) identified in 2015				
	CVE-2016-8621	cross-site scripting (XSS) identified in 2016				

	CVE-2018-1125	cross-site scripting (XSS) identified in 2018				
	CVE-2018-6759	cross-site scripting (XSS) identified in 2018				
	CVE-2020-16591	cross-site scripting (XSS) identified in 2020				
	CVE-2020-19186	cross-site scripting (XSS) identified in 2020				
	CVE-2021-46174	cross-site scripting (XSS) identified in 2021				
	CVE-2022-2206	cross-site scripting (XSS) identified in 2022				
	CVE-2022-2286	cross-site scripting (XSS) identified in 2022				
	CVE-2022-3235	cross-site scripting (XSS) identified in 2022				
	CVE-2022-4292	cross-site scripting (XSS) identified in 2022				
	CVE-2022-43552	cross-site scripting (XSS) identified in 2022				
	CVE-2023-25584	cross-site scripting (XSS) identified in 2023				
	CVE-2023-26115	buffer overflow identified in 2023				
	CVE-2023-5678	cross-site scripting (XSS) identified in 2023				
V101: Insecure Deserialization in components.						
V102: Flaws in Specific Frameworks.						
V103: Cloud Environment Misconfiguration.	CVE-2018-1000001	buffer overflow identified in 2018				
	CVE-2023-0054	privilege escalation identified in 2023				
V104: Infrastructure Tools Misconfiguration.						
V105: Mismanagement of VMs.	CVE-2020-36230	privilege escalation identified in 2020				
	CVE-2023-29499	privilege escalation identified in 2023				
V106: Insufficient Network Security.						
V107: Lack of Integration Tool Security.						
V108: CI/CD Misconfigurations.	CVE-2020-36222	privilege escalation identified in 2020				
V109: Pipeline not having Security Controls.						
V110: Vulnerable Code Deployment.						
V111: Insecure IaC Scripts.	CVE-2018-5741	privilege escalation identified in 2018				
	CVE-2023-36191	privilege escalation identified in 2023				
V112: Automated Deployment of Misconfigured Infrastructure.	CVE-2017-9047	privilege escalation identified in 2017			CVE-2021-32640	privilege escalation identified in 2021
	CVE-2019-11719	privilege escalation identified in 2019				
	CVE-2023-32665	privilege escalation identified in 2023				
V113: Secrets Hardcoded Within IaC Scripts.						
V114: No Version Control for IaC.						
V115: Insufficient Storage and Rotation of Secrets.						
V116: No Centralized Secrets Management System.						
V117: Committing Secrets in Version Control.						
V118: Failure to Monitor Secrets Access Logs.						
V119: Not Having Enough Automated Testing.						
V120: Poor/no Manual Reviews of Security.						
V121: Not Acting on Test Results.						
V122: Outdated Testing Tools Used.						
V123: No Proper Training Provided for Teams.	CVE-2017-6965	unauthorized access identified in 2017				
V124: Not Considering Security in Early Phases of Development.	CVE-2017-6966	improper access control identified in 2017				
V125: Inconsistent Security Practices Application.	CVE-2017-9049	improper access control identified in 2017				
V126: Low/Poor Collaboration Levels of Security and DevOps.	CVE-2017-8804	unauthorized access identified in 2017				