		SNYK	I	Trivy	1	OWASP DC	
Proposed Vulnerabilities	CVE Numbers	Description	CVE Numbers	Description	CVE Numbers	Description	
V1: Exposed API Endpoints without Authentication.	CVE-2021-39151	improper access control identified in 2021	CVE IVAIIIDEIS	Description	CVE IVAIIIDEIS	Description	
2. 2. posed / ii / Emaporito Widiout Authentication.	CVE-2021-39131 CVE-2023-0464	improper access control identified in 2021]				
	CVE-2023-0404 CVE-2022-42004	unauthorized access identified in 2022					
	CVE-2022-42004 CVE-2022-0529	improper access control identified in 2022					
V2: Accidental Exposure of Sensitive API Endpoints.	CVE-2022-0329 CVE-2019-1543	unauthorized access identified in 2019					
12.7. Condental Exposure of Sensitive All Litupolitis.	CVE-2019-1343 CVE-2020-1967	data leak vulnerability identified in 2020					
	CVE-2019-11727	information disclosure identified in 2019					
	CVE-2013 11727 CVE-2023-45648	data leak vulnerability identified in 2023					
	CVE-2020-15522	information disclosure identified in 2020					
	CVE-2019-8457	injection vulnerability identified in 2019					
V3: Unknown/ Untrusted APIs.	2013 0 137	and the second s					
V4: Weak authentication mechanisms for APIs.	CVE-2021-39146	improper access control identified in 2021					
	CVE-2022-40674	improper access control identified in 2022					
	CVE-2022-3996	improper access control identified in 2022					
	CVE-2020-25638	information disclosure identified in 2020					
	CVE-2018-20676	unauthorized access identified in 2018					
V5: Insecure data serialization.							
V6: Misconfiguration of API gateways.	CVE-2022-2509	improper access control identified in 2022					
3 gazana, s.	CVE-2020-24659	improper access control identified in 2020					
	CVE-2023-1370	cross-site scripting (XSS) identified in 2023					
	CVE-2016-10735	improper access control identified in 2016					
V7: Service Registration Poisoning.	CVE-2021-39152	improper access control identified in 2021					
	CVE-2022-25314	unauthorized access identified in 2022					
	CVE-2022-42011	improper access control identified in 2022					
V8: Unauthorized Access to Service Discovery.	CVE-2020-13790	improper access control identified in 2020					
	CVE-2019-3462	improper access control identified in 2019					
V9: Unavailability of Service Registration Validation.							
V10: Unauthorized Service Deregistration.	CVE-2022-38749	data leak vulnerability identified in 2022					
	CVE-2019-12290	improper access control identified in 2019					
	CVE-2020-12399	improper access control identified in 2020					
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.	CVE-2021-20305	information disclosure identified in 2021					
	CVE-2018-20843	injection vulnerability identified in 2018					
	CVE-2021-31239	information disclosure identified in 2021					
	CVE-2022-0530	data leak vulnerability identified in 2022					
	CVE-2020-29362	information disclosure identified in 2020					
	CVE-2020-26258	data leak vulnerability identified in 2020					
	CVE-2019-17023	information disclosure identified in 2019					
	CVE-2023-3446	data leak vulnerability identified in 2023					
	CVE-2021-39537	data leak vulnerability identified in 2021					
V22: Improper Encryption Key Management.	CVE-2020-35512	information disclosure identified in 2020	I				

	CVE-2019-11719	data leak vulnerability identified in 2019	I	1	I	
	CVE-2019-3842	data leak vulnerability identified in 2019				
	CVE-2013-3642 CVE-2022-3602	information disclosure identified in 2022				
	CVE-2022-3002 CVE-2023-34241	information disclosure identified in 2023				
	CVE-2021-30640	buffer overflow identified in 2021				
	CVE-2021-24031	data leak vulnerability identified in 2021				
	CVE-2021-27568	remote code execution identified in 2021				
	CVE-2020-6096	information disclosure identified in 2020				
V23: Improper Validation of Certificates.	CVE-2020-14152	information disclosure identified in 2020				
V24: Hardcoded Encryption Keys.	CVE-2021-39154	information disclosure identified in 2021				
	CVE-2022-43680	data leak vulnerability identified in 2022				
	CVE-2020-12400	information disclosure identified in 2020				
	CVE-2020-12401	improper access control identified in 2020				
	CVE-2018-5729	data leak vulnerability identified in 2018				
	CVE-2023-2650	data leak vulnerability identified in 2023				
	CVE-2020-10029	buffer overflow identified in 2020				
	CVE-2019-17543	data leak vulnerability identified in 2019				
V25: No Proper Rate Limiting.	CVE-2022-0778	denial of service identified in 2022	CVE-2016-1000027	denial of service identified in 2016	CVE-2019-18276	denial of service identified in 2019
	CVE-2020-3810	privilege escalation identified in 2020				
	CVE-2021-21346	denial of service identified in 2021				
	CVE-2021-21344	denial of service identified in 2021				
	CVE-2022-40151	denial of service identified in 2022				
	CVE-2022-22950	unauthorized access identified in 2022				
	CVE-2018-16868	remote code execution identified in 2018				
	CVE-2017-7246	denial of service identified in 2017				
	CVE-2019-12900	denial of service identified in 2019				
	CVE-2021-3326	denial of service identified in 2021				
	CVE-2019-13627	denial of service identified in 2019				
V26: Improper Handling of Suspicious.	CVE-2018-6551	denial of service identified in 2018				
	CVE-2022-27405	denial of service identified in 2022				
	CVE-2021-33560	denial of service identified in 2021				
V27: Lack of Individualized Rate Limiting.	CVE-2019-9937		CVE-2021-33037	denial of service identified in 2021		
	CVE-2020-10001	denial of service identified in 2020	CVE-2021-41079	denial of service identified in 2021		
	CVE-2021-21342	denial of service identified in 2021				
	CVE-2022-22970	data leak vulnerability identified in 2022				
	CVE-2022-2097	denial of service identified in 2022				
	CVE-2018-5710	privilege escalation identified in 2018				
	CVE-2023-36191	denial of service identified in 2023				
	CVE-2019-17006	denial of service identified in 2019				
V28: Improper Configuration of Rate Limits.	CVE-2021-45960	denial of service identified in 2021	CVE-2022-22965	denial of service identified in 2022		
visi improper comiguration of nate similar	CVE-2019-3836	denial of service identified in 2019	012 2022 22303	actual of sel vice factioned in 2022		
	CVE-2019-2180	denial of service identified in 2019				
	CVE-2014-8166	denial of service identified in 2014				
	CVE-2014-8100 CVE-2019-12900	denial of service identified in 2019				
V29: Targeted API Abuse.	CVE-2017-12000 CVE-2017-20002	denial of service identified in 2017				
v25. Taigetta Ai i Abase.	CVE-2017-20002 CVE-2020-11022	denial of service identified in 2020				
	CVE-2020-11022 CVE-2021-21348	denial of service identified in 2020				
	CVE-2021-21348 CVE-2007-5686	denial of service identified in 2021				
V20: Work or Non evictory Database Enginetics			CVE 2021 22006	information disclosure identified in 2021		
V30: Weak or Non-existent Database Encryption.	CVE-2016-2781		CVE-2021-22096	information disclosure identified in 2021		
	CVE-2017-16231	data leak vulnerability identified in 2017	CVE-2021-25329	information disclosure identified in 2021		
	CVE-2021-33574	information disclosure identified in 2021	CVE-2021-46877	information disclosure identified in 2021		
ı	CVE-2017-15088	information disclosure identified in 2017	CVE-2022-22971	information disclosure identified in 2022	1	

_	-		-		_	_
	CVE-2022-25235	information disclosure identified in 2022	CVE-2023-41080	information disclosure identified in 2023		
	CVE-2017-14062	information disclosure identified in 2017				
	CVE-2022-22965	denial of service identified in 2022				
	CVE-2019-9169	information disclosure identified in 2019				
	CVE-2022-2526	data leak vulnerability identified in 2022				
V31: Inadequate Database Hardening.	CVE-2021-4214	information disclosure identified in 2021	CVE-2020-25638	information disclosure identified in 2020	CVE-2018-14550	information disclosure identified in 2018
	CVE-2017-12652	data leak vulnerability identified in 2017	CVE-2021-30639	data leak vulnerability identified in 2021		
	CVE-2017-1000082	information disclosure identified in 2017	CVE-2023-34036	information disclosure identified in 2023		
	CVE-2018-21029	data leak vulnerability identified in 2018				
	CVE-2022-35737	information disclosure identified in 2022				
	CVE-2019-9937	information disclosure identified in 2019				
	CVE-2022-25236	information disclosure identified in 2022				
	CVE-2022-1292	data leak vulnerability identified in 2022				
	CVE-2018-18312	data leak vulnerability identified in 2018				
	CVE-2021-46848	information disclosure identified in 2021				
V32: Using Default Database Credentials.	CVE-2013-4392	data leak vulnerability identified in 2013	CVE-2020-17527	information disclosure identified in 2020	CVE-2019-8696	unauthorized access identified in 2019
	CVE-2022-23219	remote code execution identified in 2022	CVE-2021-28170	data leak vulnerability identified in 2021	CVE-2020-3898	data leak vulnerability identified in 2020
	CVE-2021-3999	information disclosure identified in 2021	CVE-2021-42550	data leak vulnerability identified in 2021	CVE-2020-15999	information disclosure identified in 2020
	CVE-2019-3844	data leak vulnerability identified in 2019	CVE-2022-22970	data leak vulnerability identified in 2022		
	CVE-2022-29458	information disclosure identified in 2022	CVE-2022-42252	information disclosure identified in 2022		
	CVE-2004-0971	data leak vulnerability identified in 2004	CVE-2023-28708	data leak vulnerability identified in 2023		
	CVE-2023-2976	data leak vulnerability identified in 2023				
	CVE-2021-43396	data leak vulnerability identified in 2021				
	CVE-2019-9936	data leak vulnerability identified in 2019				
	CVE-2023-38471	information disclosure identified in 2023				
	CVE-2021-3520	information disclosure identified in 2021				
	CVE-2017-12424	data leak vulnerability identified in 2017				
	CVE-2021-33574	information disclosure identified in 2021				
	CVE-2021-20231	information disclosure identified in 2021				
	CVE-2023-45853	injection vulnerability identified in 2023				
V33: Exposure of Sensitive Data via Error Messages.	CVE-2018-20506	data leak vulnerability identified in 2018				
	CVE-2023-1436	data leak vulnerability identified in 2023				
	CVE-2022-27405	denial of service identified in 2022				
	CVE-2020-13632	information disclosure identified in 2020				
	CVE-2020-19185	data leak vulnerability identified in 2020				
	CVE-2019-19126	data leak vulnerability identified in 2019				
V34: Non-existent Data Integrity Checks.	CVE-2010-4756	data leak vulnerability identified in 2010	CVE-2022-29885	data leak vulnerability identified in 2022	CVE-2019-6129	information disclosure identified in 2019
	CVE-2018-5730	data leak vulnerability identified in 2018	CVE-2022-38749	data leak vulnerability identified in 2022		
V35: SQL Injection.	CVE-2021-43859	injection vulnerability identified in 2021				
	CVE-2023-0767	remote code execution identified in 2023				
	CVE-2021-43466	remote code execution identified in 2021				
	CVE-2021-3996	remote code execution identified in 2021				
	CVE-2021-43527	remote code execution identified in 2021				
V36: Cross-Site Scripting (XSS).	CVE-2022-1271	, , ,	CVE-2021-31684			cross-site scripting (XSS) identified in 2023
	CVE-2019-8675	, , ,	CVE-2022-34305		CVE-2022-34903	cross-site scripting (XSS) identified in 2022
	CVE-2018-15686	, , ,	CVE-2022-38752	cross-site scripting (XSS) identified in 2022		
	CVE-2019-3829	, , ,	CVE-2023-1370	cross-site scripting (XSS) identified in 2023		
	CVE-2020-28196	, , ,	CVE-2023-38286	cross-site scripting (XSS) identified in 2023		
	CVE-2019-12749	cross-site scripting (XSS) identified in 2019				
	CVE-2018-8740	cross-site scripting (XSS) identified in 2018				
	CVE-2021-39144	cross-site scripting (XSS) identified in 2021				
	CVE-2022-23181	buffer overflow identified in 2022			l	I

	CVE-2022-3786	cross-site scripting (XSS) identified in 2022				
	CVE-2018-1000858	improper access control identified in 2018				
	CVE-2019-11922	cross-site scripting (XSS) identified in 2019				
	CVE-2021-36770	cross-site scripting (XSS) identified in 2021				
	CVE-2022-27406	remote code execution identified in 2022				
	CVE-2019-19959	cross-site scripting (XSS) identified in 2019				
	CVE-2019-19923	cross-site scripting (XSS) identified in 2019				
	CVE-2023-20873	unauthorized access identified in 2023				
	CVE-2020-15999	information disclosure identified in 2020				
	CVE-2020-27350	cross-site scripting (XSS) identified in 2020				
	CVE-2020-12049	cross-site scripting (XSS) identified in 2020				
	CVE-2019-1547	cross-site scripting (XSS) identified in 2019				
	CVE-2018-20482	cross-site scripting (XSS) identified in 2018				
	CVE-2020-12402	cross-site scripting (XSS) identified in 2020				
	CVE-2021-21350	cross-site scripting (XSS) identified in 2021				
	CVE-2023-42795	cross-site scripting (XSS) identified in 2023				
	CVE-2023-24998	cross-site scripting (XSS) identified in 2023				
	CVE-2021-22060	privilege escalation identified in 2021				
	CVE-2018-1152	privilege escalation identified in 2018				
	CVE-2023-43785	cross-site scripting (XSS) identified in 2023				
	CVE-2020-19190	cross-site scripting (XSS) identified in 2020				
	CVE-2019-25013	remote code execution identified in 2019				
	CVE-2023-4813	cross-site scripting (XSS) identified in 2023				
	CVE-2018-0735	cross-site scripting (XSS) identified in 2018				
	CVE-2018-16869	unauthorized access identified in 2018				
	CVE-2019-19645	cross-site scripting (XSS) identified in 2019				
	CVE-2022-45873	cross-site scripting (XSS) identified in 2022				
	CVE-2021-22047	cross-site scripting (XSS) identified in 2021				
	CVE-2021-22113	cross-site scripting (XSS) identified in 2021				
	CVE-2011-3374	cross-site scripting (XSS) identified in 2011				
	CVE-2021-4217	cross-site scripting (XSS) identified in 2021				
	CVE-2018-14048	cross-site scripting (XSS) identified in 2018				
	CVE-2018-1000654	cross-site scripting (XSS) identified in 2018				
	CVE-2021-36085	cross-site scripting (XSS) identified in 2021				
	CVE-2019-19882	cross-site scripting (XSS) identified in 2019				
	CVE-2019-20838	cross-site scripting (XSS) identified in 2019				
	CVE-2022-23218	cross-site scripting (XSS) identified in 2022				
	CVE-2022-1304	cross-site scripting (XSS) identified in 2022				
	CVE-2021-3997	cross-site scripting (XSS) identified in 2021				
	CVE-2022-38752	cross-site scripting (XSS) identified in 2022				
	CVE-2019-2201	cross-site scripting (XSS) identified in 2019				
	CVE-2023-31486	cross-site scripting (XSS) identified in 2023				
	CVE-2023-31439	cross-site scripting (XSS) identified in 2023				
	CVE-2022-2274	cross-site scripting (XSS) identified in 2022				
		cross-site scripting (XSS) identified in 2019				
	CVE-2022-27404	cross-site scripting (XSS) identified in 2022				
		cross-site scripting (XSS) identified in 2022				
	CVE-2018-18311	cross-site scripting (XSS) identified in 2018				
ommand Injection.	CVE-2021-26720	buffer overflow identified in 2021	CVE-2021-30640	buffer overflow identified in 2021	CVE-2020-14363	buffer overflow identified in 20
•		buffer overflow identified in 2018	CVE-2022-1471	buffer overflow identified in 2022		buffer overflow identified in 20
	CVE-2021-23840	buffer overflow identified in 2021				
		buffer overflow identified in 2020				

1	CVE-2020-11655	buffer overflow identified in 2020	1	1	1	1
	CVE-2020-13630	buffer overflow identified in 2020				
	CVE-2019-9936	data leak vulnerability identified in 2019				
	CVE-2023-43787	buffer overflow identified in 2023				
	CVE-2009-5155	improper access control identified in 2009				
	CVE-2023-5156	buffer overflow identified in 2023				
	CVE-2021-3326	denial of service identified in 2021				
	CVE-2021-36222	buffer overflow identified in 2021				
	CVE-2022-4899	buffer overflow identified in 2022				
	CVE-2023-0217	buffer overflow identified in 2023				
	CVE-2020-11501	buffer overflow identified in 2020				
	CVE-2022-29458	information disclosure identified in 2022				
	CVE-2022-26691	buffer overflow identified in 2022				
	CVE-2022-34903	cross-site scripting (XSS) identified in 2022				
	CVE-2018-18508	buffer overflow identified in 2018				
	CVE-2020-11023	buffer overflow identified in 2020				
	CVE-2023-4527	buffer overflow identified in 2023				
	CVE-2021-3502	buffer overflow identified in 2021				
	CVE-2020-35538	buffer overflow identified in 2020				
	CVE-2020-15358	buffer overflow identified in 2020				
	CVE-2022-3821	buffer overflow identified in 2022				
	CVE-2020-13529	buffer overflow identified in 2020				
	CVE-2019-17595	buffer overflow identified in 2019				
	CVE-2017-11695	buffer overflow identified in 2017				
	CVE-2019-9192	buffer overflow identified in 2019				
	CVE-2018-6829	buffer overflow identified in 2018				
	CVE-2017-11462	buffer overflow identified in 2017				
	CVE-2023-31437	buffer overflow identified in 2023				
	CVE-2019-10202	buffer overflow identified in 2019				
V38: Insecure Deserialization of Data.	CVE-2022-22825	remote code execution identified in 2022				
	CVE-2020-5421	unauthorized access identified in 2020				
	CVE-2023-29491	remote code execution identified in 2023				
V39: User Inputs Directly Accessing Objects.	CVE-2020-10878		CVE-2022-23181	buffer overflow identified in 2022	CVE-2022-22827	buffer overflow identified in 2022
	CVE-2021-3580		CVE-2023-20863	buffer overflow identified in 2023		
	CVE-2021-39147	remote code execution identified in 2021				
	CVE-2021-33560	denial of service identified in 2021				
	CVE-2023-0215	buffer overflow identified in 2023				
	CVE-2020-35525	buffer overflow identified in 2020				
	CVE-2022-41853	buffer overflow identified in 2022				
	CVE-2022-42003	improper access control identified in 2022				
	CVE-2019-5094	buffer overflow identified in 2019				
	CVE-2019-5188	buffer overflow identified in 2019				
	CVE-2018-14040	buffer overflow identified in 2018				
	CVE-2015-8985	buffer overflow identified in 2015				
	CVE-2005-2541	buffer overflow identified in 2005				
	CVE-2017-11696	buffer overflow identified in 2017				
	CVE-2020-10029	buffer overflow identified in 2020				
	CVE-2016-10739	buffer overflow identified in 2016	0.45 0004 4000			
V40: Granting Higher than Required Level of Access.	CVE-2021-21341	1	CVE-2021-43980	privilege escalation identified in 2021		
	CVE-2019-19603	privilege escalation identified in 2019				
	CVE-2023-34036	information disclosure identified in 2023				
I	CVE-2019-16168	privilege escalation identified in 2019	I	I	I	l l

1	CVE-2021-46822	buffer overflow identified in 2021	1	I
	CVE-2021-46822 CVE-2020-13943			
		privilege escalation identified in 2020		
	CVE-2023-33201	improper access control identified in 2023		
	CVE-2020-14155	injection vulnerability identified in 2020		
	CVE-2013-4235	privilege escalation identified in 2013		
	CVE-2019-1010022	l. a		
	CVE-2017-11697	privilege escalation identified in 2017		
	CVE-2021-4209	privilege escalation identified in 2021		
	CVE-2021-3711	privilege escalation identified in 2021		
V41: Credential Hardcoding in Source Code.	CVE-2021-28170	data leak vulnerability identified in 2021		
V42: Granted Privilege Exploitation.	CVE-2019-15903	privilege escalation identified in 2019	CVE-2021-22118	privilege escalation identified in 2021
	CVE-2021-39149	improper access control identified in 2021		
	CVE-2019-19880	privilege escalation identified in 2019		
	CVE-2022-46908	privilege escalation identified in 2022		
	CVE-2019-2228	injection vulnerability identified in 2019		
	CVE-2021-21347	privilege escalation identified in 2021		
	CVE-2022-1471	buffer overflow identified in 2022		
	CVE-2015-9251	privilege escalation identified in 2015		
	CVE-2016-10739	buffer overflow identified in 2016		
	CVE-2018-14550	information disclosure identified in 2018		
	CVE-2017-18078	privilege escalation identified in 2017		
V43: Race Condition Exploitation.	CVE-2021-27645	unauthorized access identified in 2021		
V44: Improper Data Transaction Management.	CVE-2019-20386	unauthorized access identified in 2019		
V45: Insecure Data Synchronization.				
V46: Concurrent Data Access Mismanagement.	CVE-2023-44487	denial of service identified in 2023		
Ţ	CVE-2018-16865	denial of service identified in 2018		
	CVE-2020-13777	information disclosure identified in 2020		
V47: Lack of Regular Backups.	CVE-2021-3998	data leak vulnerability identified in 2021		
	CVE-2021-3450	data leak vulnerability identified in 2021		
	CVE-2021-22096	information disclosure identified in 2021		
	CVE-2020-13631	data leak vulnerability identified in 2020		
	CVE-2018-20796	information disclosure identified in 2018		
V48: Insecure Backup Storage.	CVE-2023-20883	injection vulnerability identified in 2023		
The model of Suchap Storage	CVE-2023-4911	information disclosure identified in 2023		
V49: Lack of Backup Validation.	CVE-2022-45693	information disclosure identified in 2022		
V50: Improper Disposal of Outdated Backups.	CVE-2022-45053	unauthorized access identified in 2022		
V51: Insecure/Weak Authentication.	CVE-2022-23837 CVE-2020-10543	unauthorized access identified in 2020		
VOL. INSCORIC, Weak Authentication.	CVE-2020-10343 CVE-2022-1304	cross-site scripting (XSS) identified in 2022		
	CVE-2019-19925	unauthorized access identified in 2019		
	CVE-2019-19923 CVE-2021-29505	unauthorized access identified in 2019		
	CVE-2021-23303 CVE-2020-17527	information disclosure identified in 2020		
	CVE-2020-17327 CVE-2023-20863	buffer overflow identified in 2023		
	CVE-2022-25647 CVE-2019-11358	improper access control identified in 2022 improper access control identified in 2019		
	CVE-2019-11338 CVE-2018-16869	unauthorized access identified in 2018		
VEQ: Enumeration of Associate				
V52: Enumeration of Accounts.	CVE-2023-34969	unauthorized access identified in 2023		
V53: Continued Usage of Breached Credentials.	CVE-2018-6942	unauthorized access identified in 2018		
V54: Identity Federation Misconfiguration.	CVE-2019-11745	remote code execution identified in 2019		
	CVE-2020-1712	injection vulnerability identified in 2020		
	CVE-2021-43618	injection vulnerability identified in 2018		
	CVE-2019-7309	unauthorized access identified in 2019		
I	CVE-2021-35942	denial of service identified in 2021	I	I

1	CVE-2019-19244	improper access control identified in 2019	I		1	1
V55: Provision of Higher Privileges.	CVE-2019-5827	privilege escalation identified in 2019	CVE-2020-36518	privilege escalation identified in 2020	CVE-2020-3810	privilege escalation identified in 2020
	CVE-2020-3898	data leak vulnerability identified in 2020	CVE-2021-22060	privilege escalation identified in 2021		, ,
	CVE-2021-41079	denial of service identified in 2021				
	CVE-2021-25329	information disclosure identified in 2021				
	CVE-2023-0216	privilege escalation identified in 2023				
	CVE-2023-0286	privilege escalation identified in 2023				
	CVE-2023-31484	privilege escalation identified in 2023				
	CVE-2021-33910	privilege escalation identified in 2021				
	CVE-2020-26259	privilege escalation identified in 2020				
	CVE-2021-24122	improper access control identified in 2021				
	CVE-2023-20861	injection vulnerability identified in 2023				
	CVE-2022-40149	privilege escalation identified in 2022				
	CVE-2019-1551	unauthorized access identified in 2019				
	CVE-2019-8331	privilege escalation identified in 2019				
	CVE-2019-13627	denial of service identified in 2019				
	CVE-2023-1255	privilege escalation identified in 2023				
	CVE-2021-3997	cross-site scripting (XSS) identified in 2021				
	CVE-2020-29562	privilege escalation identified in 2020				
	CVE-2017-6519	privilege escalation identified in 2017				
	CVE-2022-31782	privilege escalation identified in 2022				
	CVE-2018-7169	privilege escalation identified in 2018				
	CVE-2019-1010023	1				
	CVE-2017-11698	privilege escalation identified in 2017				
	CVE-2017-11164	privilege escalation identified in 2017				
	CVE-2011-3389	privilege escalation identified in 2011				
	CVE-2019-3843	privilege escalation identified in 2019				
	CVE-2018-9234	privilege escalation identified in 2018				
	CVE-2023-31438	privilege escalation identified in 2023				
	CVE-2022-1664	privilege escalation identified in 2022				
	CVE-2021-20232	privilege escalation identified in 2021				
V56: Improper Token Invalidation.						
V57: Insecure Access Token Storage.	CVE-2021-39150	data leak vulnerability identified in 2021				
	CVE-2021-3999	information disclosure identified in 2021				
	CVE-2022-40152	data leak vulnerability identified in 2022				
	CVE-2022-40159	data leak vulnerability identified in 2022				
	CVE-2018-14498	privilege escalation identified in 2018				
	CVE-2018-20677	information disclosure identified in 2018				
	CVE-2023-0466	unauthorized access identified in 2023				
	CVE-2019-18276	denial of service identified in 2019				
	CVE-2021-20193	data leak vulnerability identified in 2021				
	CVE-2018-5709	information disclosure identified in 2018				
V58: Embedded Static Credentials.	CVE-2021-46143	remote code execution identified in 2021				
	CVE-2021-39139	remote code execution identified in 2021				
	CVE-2022-3479	remote code execution identified in 2022				
	CVE-2020-1971	remote code execution identified in 2020				
	CVE-2021-3468	remote code execution identified in 2021				
	CVE-2019-6454	remote code execution identified in 2019				
	CVE-2023-0465	remote code execution identified in 2023				
V59: Reuse of Passwords.	CVE-2022-4415	improper access control identified in 2022	CVE-2022-42004	unauthorized access identified in 2022	CVE-2019-6488	improper access control identified in 2019
	CVE-2023-2975	improper access control identified in 2023				
1	CVE-2021-45346	unauthorized access identified in 2021			1	

Comparison Com	-	_				_	
Commonweight Comm		CVE-2013-0340	improper access control identified in 2013	1			
Display Disp			1 ' '	1			
District Control Con				1			
Over 2007-1932-34 Control Cont	V60: Vulnerable Password Recovery Process.		1 ' '	1			
CV - 2019 - 1942 CV - 2019 -	V61: MFA not Used/Enforced.			1			
C2-Phi-him gatasis on Users C3-2-Phi-him gatasis on Users C3-2-Phi-him gatasis on Users C3-2-Phi-him gatasis on Users C3-2-Phi-him gatasis of C3-2-Phi-him gatasis o			1 ' '	1			
Section CV-2019-9896 CV-2019-9							1
Over-2012-14588 Over-2012-14598 Over-2012-14598 Over-2012-14599 Over-2012-	V62: Phishing Attacks on Users.	CVE-2019-19242	unauthorized access identified in 2019	1			
Over-2021-24590 (CV-2021-24590 (CV-2	V63: Unenforced Access Controls.						1
CVF-2007-25488 CVF-2007-25498 CVF-2007-25499 CVF-			privilege escalation identified in 2022	1			
CV-2021-21349 CV-2021-2036 CV-		CVE-2023-26604	unauthorized access identified in 2023	1			
CV-2002-13856 CV-2013-1456 CV-2002-13871 CV-2002-13871 CV-2002-13872 CV-2002-13872 CV-2002-13873							1
CUF-2017-2986 CUF-2017-298		CVE-2021-21349	unauthorized access identified in 2021	1			
64: Human Error in Granting Access. (VE-2013-1866) (VE-2013-2877) (VE-2012-2826) (VE-2012-2826) (VE-2012-2826) (VE-2012-2826) (VE-2012-2826) (VE-2012-2827) (VE-2012-28282) (VE		CVE-2020-13956	improper access control identified in 2020	1			
## Authorities ducess CV-2011-4115 CV-2021-3143 CV-2021-3143		CVE-2022-22968	injection vulnerability identified in 2022	1			
Authorited access identified in 2021 Ox-2002-18286 Ox-2002-28286 Ox-2002-283751 O		CVE-2018-16866	privilege escalation identified in 2018				
St. insecure Direct Object Reference. CVF-7007-2978b CVF-2022-2978b CVF-2022-297	V64: Human Error in Granting Access.	CVE-2011-4116	unauthorized access identified in 2011	1			
Section Company Comp		CVE-2023-38472	unauthorized access identified in 2023	1			
CF-2012-22193		CVE-2020-12403	unauthorized access identified in 2020	1			
CVE-2012-338761 CVE-2012-31818 CVE-2012-31818 CVE-2012-31818 CVE-2012-34016 CVE-2018-2012 CVE-2012-34016	V65: Insecure Direct Object Reference.	CVE-2022-22826	buffer overflow identified in 2022	CVE-2021-27568	remote code execution identified in 2021	CVE-2019-11745	remote code execution identified in 2019
CVE. 2021 - 22118 CVE. 2022 - 22119 CVE. 2022 - 22118 CVE. 2022 - 22119 CVE. 2		CVE-2022-22976	remote code execution identified in 2022	1			
CVE-2012-4015 cmrolt code execution identified in 2018 cvE-2018-1049 c		CVE-2022-38751	privilege escalation identified in 2022	1			
CVE-2018-1049 CVE-2018-20217 CVE-2012-29423 CVE-2012-29423 CVE-2022-29404 CVE-2020-27618 CVE-2022-24304 CVE-2020-27618 CVE-2022-24305 CVE-2022-24306 CVE-2022-24306 CVE-2022-24307 CVE-2022-24307 CVE-2022-24307 CVE-2022-24307 CVE-2022-24308 CVE-2019-16924 CVE-2022-24308 CVE-2019-16925 CVE-2019-16925 CVE-2019-16925 CVE-2019-1695 CVE-2019-1695 CVE-2019-1695 CVE-2019-1695 CVE-2019-1695 CVE-2019-1695 CVE-2019-1695 CVE-2019-1695 CVE-2019-1695 CVE-2019-1696 CVE-2019-25013		CVE-2021-22118	privilege escalation identified in 2021	1			
CVF-2012-1925		CVE-2022-40150	remote code execution identified in 2022	1			
CVE-2021-24251 remote code execution identified in 2021 remote code execution identified in 2020 remote code execution identified in 2019 remote code execution identified in 2021 remote code execution identified in 2022 remote code execution		CVE-2018-1049	remote code execution identified in 2018	1			
CVE-2022-42010 remote code execution identified in 2022 remote code execution identified in 2023 remote code execution identified in 2021 remote code execution identified in 2022 remote		CVE-2018-20217	injection vulnerability identified in 2018	1			
CVF-2002-4304 remote code execution identified in 2020 remote code execution identified in 2021 remote code execution identified in 2021 remote code execution identified in 2015 remote code execution identified in 2016 remote code execution identified in 2016 remote code execution identified in 2018 remote code execution identified in 2022 remote code execution i		CVE-2021-29425	remote code execution identified in 2021	1			
CVE-202-4304 CVE-2020-27618 CVE-2020-27618 CVE-2021-4797 CVE-2019-19924 CVE-2019-19924 CVE-2019-19855 remote code execution identified in 2019 CVE-2018-16805 CVE-2018-1969 CVE-2018-16969 CVE-2018-16868 CVE-2022-27466 CVE-2019-25013 CVE-2018-16868 CVE-2012-36868 CVE-2012-38919 CVE-2018-16868		CVE-2022-42010	remote code execution identified in 2022	1			
CVE-202-24786 CVE-2019-19924 CVE-2019-19924 CVE-2019-19924 CVE-2019-19924 CVE-2019-19924 CVE-2019-19924 CVE-2019-19924 CVE-2019-19924 CVE-2019-19924 CVE-2019-19925 CVE-2019-19925 CVE-2019-14855 CVE-2019-14855 CVE-2019-14855 CVE-2019-1690 CVE-2021-37600 CVE-2021-37600 CVE-2019-19916 CVE-2018-6485 CVE-2019-1996 CVE-2018-6485 CVE-2022-2406 CVE-2022-25648 CVE-2022-2565 CVE-2022-48503 CVE-2022-28520 CVE-2022-22550 CVE-2022-22		CVE-2020-19187	remote code execution identified in 2020	1			
CVE-2020-24736 remote code execution identified in 2020 remote code execution identified in 2021 remote code execution identified in 2019 remote code execution identified in 2021 remote code execution identified in 2019 remote code execution identified in 2022 remote code execution		CVE-2022-4304	remote code execution identified in 2022	1			
CVE-2019-19924 CVE-2019-19924 CVE-2019-19825 CVE-2016-10228 CVE-2016-10228 CVE-2019-1969 CVE-2019-9169 CVE-2019-9169 CVE-2019-1685 CVE-2019-9169 CVE-2019-9169 CVE-2018-6485 CVE-2022-27406 CVE-2019-1865 CVE-2022-27406		CVE-2020-27618	denial of service identified in 2020	1			
CVE-2013-1679 CVE-2019-14855 CVE-2016-10228 CVE-2013-7600 CVE-2021-37600 CVE-2022-3563 CVE-2019-9169 CVE-2018-6485 CVE-2022-27406 CVE-2022-27406 CVE-2022-27406 CVE-2018-6485 CVE-2019-5013 CVE-2018-6485 CVE-2019-5048 CVE-2018-16868 CVE-2019-5048 CVE-2018-16868 CVE-2018-16868 CVE-2018-16868 CVE-2018-16868 CVE-2018-16868 CVE-2018-16868 CVE-2018-28322 CVE-2018-28323 CVE-2018-28324 CVE-2018-28334 CVE-2018-28334 CVE-2018-28344 CVE-2018-28344 CVE-2018-28345 C		CVE-2020-24736	remote code execution identified in 2020	1			
CVE-2019-14855 CVE-2019-14855 CVE-2019-14855 CVE-2019-2503 remote code execution identified in 2019 remote code execution identified in 2021 remote code execution identified in 2021 remote code execution identified in 2021 remote code execution identified in 2019 remote code execution identified in 2020 remote code execution identified in 2021 remote code execution identified in 2022 remote code executi		CVE-2019-19924	remote code execution identified in 2019	1			
CVE-2013-17600 CVE-2022-20563 CVE-2019-9169 CVE-2018-6485 CVE-2022-27406 CVE-2022-27406 CVE-2022-27406 CVE-2019-9169 CVE-2018-6485 CVE-2019-9169 CVE-2018-6485 CVE-2019-9169 CVE-2018-6485 CVE-2019-95013 CVE-2019-95013 CVE-2018-16868 CVE-2019-25013 CVE-2018-16868 CVE-2019-25013 CVE-2018-16868 CVE-2022-48522 CVE-2022-48520 CVE-2022-48520 CVE-2022-48520 CVE-2022-48520 CVE-2022-48520 CVE-2022-3319 CVE-2022-3319 CVE-2022-3319 CVE-2022-3385 CVE-2022-23852 Unauthorized access identified in 2022 CVE-2022-24252 information identified in 2022 information identified in 2021 cremote code execution identified in 2018 remote code execution identified in 2018 remote code execution identified in 2022		CVE-2022-31679	remote code execution identified in 2022	1			
CVE-2021-37600 CVE-2022-0563 CVE-2019-9169 CVE-2018-6485 CVE-2022-27406 CVE-2020-25648 CVE-2019-25048 CVE-2019-25048 CVE-2019-25048 CVE-2019-25048 CVE-2019-25048 CVE-2019-25049 CVE-2019-26049 CVE-2019-		CVE-2019-14855	remote code execution identified in 2019	1			
CVE-2022-0563 CVE-2019-9169 CVE-2018-6485 CVE-2022-27406 CVE-2022-27406 CVE-2019-25013 CVE-2019-25013 CVE-2019-25013 CVE-2018-16868 CVE-2019-25013 CVE-2018-2689 CVE-2019-25013 CVE-2018-2689 CVE-2018-2689 CVE-2019-25013 CVE-2018-2689 CVE-2018-2689 CVE-2019-25013 CVE-2018-2689 CVE-20		CVE-2016-10228	remote code execution identified in 2016	1			
CVE-2019-9169 CVE-2018-6485 CVF-2022-27406 CVF-2022-27406 CVF-2022-27406 CVF-2022-27407 CVF-2022-27407 CVF-2022-27407 CVF-2022-27407 CVF-2022-27408 CVF-2019-9169 CVF-2019-9169 CVF-2018-6485 CVF-2019-25013 remote code execution identified in 2022 remote code execution identified in 2019 remote code execution identified in 2019 remote code execution identified in 2018 remote code execution identified in 2022 remote code execution identified in 2		CVE-2021-37600	remote code execution identified in 2021	1			
CVE-2018-6485 remote code execution identified in 2018 remote code execution identified in 2022 remote code execution identified in 2020 remote code execution identified in 2020 remote code execution identified in 2019 remote code execution identified in 2019 remote code execution identified in 2018 remote code execution identified in 2022 remote code execution i		CVE-2022-0563	remote code execution identified in 2022	1			
CVE-2022-27406 CVE-2020-25648 CVE-2019-25013 CVE-2019-25013 CVE-2018-16868 CVE-2022-48522 CVE-2022-48303 CVE-2022-23219 CVE-2022-23219 CVE-2022-23219 CVE-2022-23219 CVE-2022-23223 CVE-2022-23852 CVE-2022-23852 CVE-2022-23852 CVE-2022-42525 CVE-2022-4252 CVE-2022-4252 CVE-2022-4252 CVE-2022-4252 CVE-2022-4252 CVE-2022-4252 CVE-2022-4252 CVE-2022-22852 CVE-2022-4252 CVE-2022-4252 CVE-2022-22852 CVE-2022-22852 CVE-2022-42252 CVE-2022-42252 CVE-2022-42252 CVE-2022-42252 CVE-2022-42252 CVE-2022-22950		CVE-2019-9169	information disclosure identified in 2019	1			
CVE-2020-25648 CVE-2019-25013 remote code execution identified in 2020 remote code execution identified in 2019 remote code execution identified in 2018 cVE-2022-48522 remote code execution identified in 2022 improper access control identified in 2022 unauthorized access identified in 2022 unauthorized access identified in 2022 information disclosure identified in 2022 unauthorized access		CVE-2018-6485	remote code execution identified in 2018	1			
CVE-2019-25013 remote code execution identified in 2019 remote code execution identified in 2018 remote code execution identified in 2018 remote code execution identified in 2022 remote code execution		CVE-2022-27406	remote code execution identified in 2022	1			
CVE-2018-16868 CVE-2022-48522 remote code execution identified in 2018 remote code execution identified in 2022 remote		CVE-2020-25648	remote code execution identified in 2020	1			
CVE-2022-48522 remote code execution identified in 2022 improper access control identified in 2018 unauthorized access identified in 2022 unauthorized access identified in 2022 remote code execution identified in 2022 improper access control identified in 2021 code execution identified in 2022 improper access control identified in 2021 remote code execution identified in 2022 improper access control identified in 2021 code execution identified in 2022 improper access control identified in 2021 code execution identified in 2022 improper access control identified in 2021 code execution identified in 2022 improper access control identified in 2021 code execution identified in 2022 improper access control identified in 2021 code execution identified in 2022 improper access control identified in 2021 code execution identified in 2022 improper access control identified in 2021 code execution identified in 2022 improper access control identified in 2021 code execution identified in 2022 improper access control identified in 2021 code execution identified in 2021 code execution identified in 2022 improper access control identified in 2021 code execution identified in 2021 code execution identified in 2022 improper access control identified in 2021 code execution identified in 2021 code execution identified in 2022 improper access control identified in 2021 code execution identified in 2021 code execution identified in 2022 improper access control identified in 2021 code execution identified in 2021 code execution identified in 2022 improper access control identified in 2021 code execution identified in 2022 improper access control identified in 2021 code execution identified in 2022 improper acces		CVE-2019-25013	remote code execution identified in 2019				
CVE-2022-48303 remote code execution identified in 2022 remote code execution identified in 2022 remote code execution identified in 2022 improper access control identified in 2022 unauthorized access identified in 2022 unauthorized access identified in 2022 remote code execution identified in 2022 improper access control identified in 2021 improper access control identified in 2020 unauthorized access identified in 2022 unauthorized access identified in 2022 information disclosure identified in 2022 unauthorized access		CVE-2018-16868	remote code execution identified in 2018	1			
CVE-2022-23219 remote code execution identified in 2022 improper access control identified in 2022 cVE-2018-12384 CVE-2022-22823 cVE-2022-23852 cVE-2022-42252 information disclosure identified in 2022 control identified in 2021 control identified in 2022 control i		CVE-2022-48522	remote code execution identified in 2022	1			
CVE-2022-23219 remote code execution identified in 2022 improper access control identified in 2022 cVE-2018-12384 CVE-2022-22823 cVE-2022-23852 cVE-2022-42252 information disclosure identified in 2022 control identified in 2021 control identified in 2022 control i		CVE-2022-48303	remote code execution identified in 2022	1			
improper access control identified in 2018 CVE-2021-24122 improper access control identified in 2021 CVE-2020-13790 improper access control identified in 2020 improper access control identified in 2022 information disclosure identified in 2022 cVE-2022-22950 improper access control identified in 2022 information disclosure identified in 2022 cVE-2022-22950 improper access control identified in 2021 improper access control identified in 2021 cVE-2020-13790 improper access control identified in 2020 improper access control identified in 2021 cVE-2020-13790 improper access control identified in 2020 improper access control identified in 2021 cVE-2020-13790 improper access control identified in 2020 improper access control identified in 2021 cVE-2020-13790 improper access control identified in 2020 improper access control identified in 2021 cVE-2020-13790 improper access control identified in 2020 improper access control identified in 2021 cVE-2020-13790 improper access control identified in 2020 improper access control identified in 2021 cVE-2020-13790 improper access control identified in 2020 improper access control identified in 2021 cVE-2020-13790 improper				1			
CVE-2022-22823 unauthorized access identified in 2022 CVE-2022-23852 unauthorized access identified in 2022 information disclosure identified in 2022 CVE-2022-22950 unauthorized access identified in 2022	V66: Vulnerable APIs Having Higher Control.			CVE-2021-24122	improper access control identified in 2021	CVE-2020-13790	improper access control identified in 2020
CVE-2022-23852 unauthorized access identified in 2022 CVE-2022-42252 information disclosure identified in 2022 CVE-2022-22950 unauthorized access identified in 2022			· ·				' '
67: Session Hijacking. CVE-2022-42252 information disclosure identified in 2022 CVE-2022-22950 unauthorized access identified in 2022				1			
	V67: Session Hijacking.			CVE-2022-22950	unauthorized access identified in 2022		
	, 3						
	•	•				•	•

1	CVE-2023-38286	cross-site scripting (XSS) identified in 2023	ı	1	ı	1
V68: Cross-Site Request Forgery.	CVE-2018-0734		CVE-2020-17521	unauthorized access identified in 2020		
voo. cross site nequest rongery.	CVE-2019-15718	unauthorized access identified in 2019	CVE-2022-42003	improper access control identified in 2022		
	CVE-2019-1010024	unauthorized access identified in 2019	012 2022 12000	mproper access control acritimea in 2022		
	CVE-2018-1000858	improper access control identified in 2018				
	CVE-2020-1751	unauthorized access identified in 2020				
	CVE-2020-1752	unauthorized access identified in 2020				
	CVE-2020-35527	improper access control identified in 2020				
V69: Session Control Exploitation.	CVE-2018-4300	unauthorized access identified in 2018	CVE-2020-5421	unauthorized access identified in 2020	CVE-2022-22747	unauthorized access identified in 2022
Proprietation	CVE-2021-31684		CVE-2023-20873	unauthorized access identified in 2023	012 2022 227 17	andamented decess racinimed in 2022
	CVE-2020-17541	improper access control identified in 2020	012 2023 20073	and deficition and deficition and an arrangement and arrangement and arrangement arrangeme		
	CVE-2020-16156	improper access control identified in 2020				
V70: Improper Session Expiry.	CVE-2023-4806	1	CVE-2022-25857	unauthorized access identified in 2022	CVF-2021-40528	unauthorized access identified in 2021
V70. Improper Session Expiry.	CVE-2019-1549	improper access control identified in 2019	CVL 2022 23037	diludeilotized decess identified iii 2022	CVL 2021 40320	undunonized decess identified in 2021
	CVE-2019-17594	improper access control identified in 2019				
	CVE-2018-1000001	unauthorized access identified in 2018				
	CVE-2016-2779	improper access control identified in 2016				
	CVE-2010-2775	denial of service identified in 2022				
V71: Container Misconfigurations.	CVL 2022 41054	definal of service identified in 2022				
V72: Improper Container Isolation.						
V73: Direct Storage of Sensitive Data on Container Image.	CVE-2021-22053	information disclosure identified in 2021				
	CVE-2021-21343	information disclosure identified in 2021				
	CVE-2020-13776	denial of service identified in 2020				
	CVE-2019-13232	information disclosure identified in 2019				
V74: Outdated/Insecure Container Image Usage.						
V75: Misconfiguration of Orchestration Dashboards.						
V76: Orchestration Tools Having Unrestricted API Access.	CVE-2019-3844	data leak vulnerability identified in 2019				
V77: Poor Definition of RBAC.	CVE-2018-12886	privilege escalation identified in 2018				
	CVE-2019-5018	privilege escalation identified in 2019				
	CVE-2018-16864	privilege escalation identified in 2018				
	CVE-2022-25313	improper access control identified in 2022				
	CVE-2021-33037	denial of service identified in 2021				
	CVE-2023-28708	data leak vulnerability identified in 2023				
	CVE-2021-36084	privilege escalation identified in 2021				
	CVE-2019-1010025	improper access control identified in 2019				
	CVE-2023-4641	privilege escalation identified in 2023				
	CVE-2023-38469	privilege escalation identified in 2023				
V78: Vulnerabilities in Orchestration Tools.	CVE-2018-20346	remote code execution identified in 2018				
	CVE-2020-1751	unauthorized access identified in 2020				
	CVE-2021-37750	remote code execution identified in 2021				
	CVE-2022-37434	remote code execution identified in 2022				
V79: Insecure Service Configuration.	CVE-2018-25032	denial of service identified in 2018				
V80: Service Deployments with no Configuration Validation.	CVE-2020-36518	privilege escalation identified in 2020				
	CVE-2023-0401	unauthorized access identified in 2023				
	CVE-2020-1752	unauthorized access identified in 2020				
V81: Embedded Passwords/Tokens in Configuration Files.	CVE-2020-12723	information disclosure identified in 2020	CVE-2022-38751	privilege escalation identified in 2022		
	CVE-2021-39141	information disclosure identified in 2021				
	CVE-2020-17521	unauthorized access identified in 2020				
	CVE-2021-4160	data leak vulnerability identified in 2021				
	CVE-2020-6829	improper access control identified in 2020				
	CVE-2018-14042	data leak vulnerability identified in 2018				
	CVE-2017-7245	information disclosure identified in 2017				
•	•	•	•	•	-	•

•				1		_
V82: Insecure Configuration File Validation.	CVE-2021-3995	remote code execution identified in 2021				
	CVE-2022-4203	remote code execution identified in 2022				
	CVE-2021-24032	remote code execution identified in 2021				
	CVE-2019-8842	remote code execution identified in 2019				
	CVE-2021-36086	remote code execution identified in 2021				
	CVE-2007-6755	remote code execution identified in 2007				
	CVE-2022-38750	improper access control identified in 2022				
	CVE-2020-15250	remote code execution identified in 2020				
	CVE-2019-18224	remote code execution identified in 2019				
V83: Adding Components with Known Vulnerabilities.	CVE-2021-3712	information disclosure identified in 2021				
	CVE-2023-4504	remote code execution identified in 2023				
	CVE-2023-3138	unauthorized access identified in 2023				
V84: Outdated/Unmaintained Dependency Usage.	CVE-2019-2201	cross-site scripting (XSS) identified in 2019				
	CVE-2021-43980	privilege escalation identified in 2021				
V85: Insufficient Scanning of Dependencies.	CVE-2019-3843	privilege escalation identified in 2019				
V86: No Transitive Dependency Validation.	CVE-2019-20218	privilege escalation identified in 2019				
	CVE-2022-42898	privilege escalation identified in 2022				
	CVE-2018-12404	denial of service identified in 2018				
	CVE-2018-11813	privilege escalation identified in 2018				
	CVE-2021-36690	privilege escalation identified in 2021				
	CVE-2018-1152	privilege escalation identified in 2018				
	CVE-2018-14498	privilege escalation identified in 2018				
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.	CVE-2020-13871	denial of service identified in 2020	CVE-2022-41854	denial of service identified in 2022	CVE-2020-13776 de	enial of service identified in 2020
, -	CVE-2018-19591	denial of service identified in 2018				
	CVE-2022-4450	denial of service identified in 2022				
	CVE-2021-35942	denial of service identified in 2021				
V95: Compromised Supply Chain Attacks.						
V96: Third-Party Components Service Outages.	CVE-2021-39145	denial of service identified in 2021				
	CVE-2020-27618	denial of service identified in 2020				
	CVE-2019-9893	denial of service identified in 2019				
	CVE-2023-38470	denial of service identified in 2023				
	CVE-2022-22824	denial of service identified in 2022				
	CVE-2021-31535	denial of service identified in 2021				
V97: Insecure Third-Party Components.	CVE-2022-22827	buffer overflow identified in 2022				
	CVE-2019-17007	injection vulnerability identified in 2019				
	CVE-2021-39153	remote code execution identified in 2021				
	CVE-2020-9327	remote code execution identified in 2020				
	CVE-2021-40528	unauthorized access identified in 2021				
	CVE-2021-23841	unauthorized access identified in 2021				
V98: No Proper Security Practices in Third-Party Components.						
V99: Various Injection Vulnerabilities.	CVE-2022-23990	remote code execution identified in 2022	CVE-2021-25122	injection vulnerability identified in 2021	CVE-2023-45853 in	jection vulnerability identified in 2023
	CVE-2021-39148	injection vulnerability identified in 2021	CVE-2022-22968	injection vulnerability identified in 2022		ijection vulnerability identified in 2020
	CVE-2022-3715	injection vulnerability identified in 2022	CVE-2023-20861	injection vulnerability identified in 2023	I	jection vulnerability identified in 2018
	CVE-2020-16156	improper access control identified in 2020	CVE-2023-20883	injection vulnerability identified in 2023		jection vulnerability identified in 2018
	CVE-2020-14344	injection vulnerability identified in 2020		, , , , , , , , , , , , , , , , , , , ,	I	jection vulnerability identified in 2019
•	•	1 -	•	ī	• '	•

_	_		_	_	
	CVE-2022-22747	unauthorized access identified in 2022		CVE-2019-2228	injection vulnerability identified in 2019
	CVE-2020-13434	injection vulnerability identified in 2020			
	CVE-2019-7317	injection vulnerability identified in 2019			
	CVE-2021-39140	injection vulnerability identified in 2021			
	CVE-2021-21345	injection vulnerability identified in 2021			
	CVE-2023-41080	information disclosure identified in 2023			
	CVE-2021-46877	information disclosure identified in 2021			
	CVE-2021-25122	injection vulnerability identified in 2021			
	CVE-2022-40160	injection vulnerability identified in 2022			
	CVE-2023-43786	injection vulnerability identified in 2023			
	CVE-2020-19186	injection vulnerability identified in 2020			
	CVE-2020-19189	injection vulnerability identified in 2020			
	CVE-2020-19188	injection vulnerability identified in 2020			
	CVE-2021-3449	injection vulnerability identified in 2021			
	CVE-2023-1981	injection vulnerability identified in 2023			
	CVE-2023-32360	injection vulnerability identified in 2023			
	CVE-2020-13435	injection vulnerability identified in 2020			
	CVE-2021-20227	injection vulnerability identified in 2021			
	CVE-2023-3817	injection vulnerability identified in 2023			
	CVE-2023-3817 CVE-2020-11656	injection vulnerability identified in 2020			
	CVE-2020-11030 CVE-2019-6488	improper access control identified in 2019			
	CVE-2019-0488 CVE-2019-9923	injection vulnerability identified in 2019			
	CVE-2019-9923 CVE-2019-6129	information disclosure identified in 2019			
	CVE-2021-36087	injection vulnerability identified in 2021			
	CVE-2010-0928	injection vulnerability identified in 2010			
	CVE-2017-18018	injection vulnerability identified in 2017			
	CVE-2022-27404	cross-site scripting (XSS) identified in 2022			
	CVE-2018-6954	injection vulnerability identified in 2018			
	CVE-2017-12132	injection vulnerability identified in 2017			
	CVE-2020-14155	injection vulnerability identified in 2020			
	CVE-2018-16888	injection vulnerability identified in 2018			
	CVE-2020-8908	injection vulnerability identified in 2020			
	CVE-2022-3219	injection vulnerability identified in 2022			
	CVE-2023-0634	injection vulnerability identified in 2023			
	CVE-2023-4421	injection vulnerability identified in 2023			
	CVE-2018-20217	injection vulnerability identified in 2018			
	CVE-2023-29383	injection vulnerability identified in 2023			
	CVE-2023-38473	injection vulnerability identified in 2023			
	CVE-2022-22822	injection vulnerability identified in 2022			
	CVE-2022-25315	injection vulnerability identified in 2022			
	CVE-2022-2068	injection vulnerability identified in 2022			
	CVE-2019-8457	injection vulnerability identified in 2019			
V100: Improper XSS Prevention Implementation.					
V101: Insecure Deserialization in components.					
V102: Flaws in Specific Frameworks.					
V103: Cloud Environment Misconfiguration.					
V104: Infrastructure Tools Misconfiguration.					
V105: Mismanagement of VMs.					
V106: Insufficient Network Security.					
V107: Lack of Integration Tool Security.					
V108: CI/CD Misconfigurations.					
V109: Pipeline not having Security Controls.	1			I	

V110: Vulnerable Code Deployment.			
V111: Insecure IaC Scripts.	CVE-2020-14363	buffer overflow identified in 2020	
V112: Automated Deployment of Misconfigured Infrastructure.			
V113: Secrets Hardcoded Within IaC Scripts.	CVE-2020-26217	information disclosure identified in 2020	
	CVE-2023-0361	information disclosure identified in 2023	
	CVE-2022-41966	information disclosure identified in 2022	
	CVE-2022-42012	information disclosure identified in 2022	
	CVE-2017-15232	privilege escalation identified in 2017	
	CVE-2018-19211	data leak vulnerability identified in 2018	
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.	CVE-2019-11729	information disclosure identified in 2019	
	CVE-2022-3358	information disclosure identified in 2022	
	CVE-2019-10172	data leak vulnerability identified in 2019	
	CVE-2019-1563	data leak vulnerability identified in 2019	
	CVE-2017-13685	data leak vulnerability identified in 2017	
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.			
V124: Not Considering Security in Early Phases of Development.			
V125: Inconsistent Security Practices Application.			
V126: Low/Poor Collaboration Levels of Security and DevOps.			