| Proposed Vulnerabilities | SNYK | | Trivy | | OWASP DC | |
|---|---|---|---|---|---|---|
| | CVE Numbers | Description | CVE Numbers | Description | CVE Numbers | Description |
| V1: Exposed API Endpoints without Authentication. | CVE-2018-19362 | improper access control identified in 2018 | | | | |
| | CVE-2021-21349 | improper access control identified in 2021 | | | | |
| V2: Accidental Exposure of Sensitive API Endpoints. | CVE-2023-44487 | data leak vulnerability identified in 2023 | | | | |
| V3: Unknown/ Untrusted APIs. | | | | | CVE-2019-20330 | improper access control identified in 2019 |
| V4: Weak authentication mechanisms for APIs. | CVE-2020-10969 | improper access control identified in 2020 | | | | |
| | CVE-2021-39139 | unauthorized access identified in 2021 | | | | |
| V5: Insecure data serialization. | | | | | CVE-2021-43795 | denial of service identified in 2021 |
| V6: Misconfiguration of API gateways. | | | | | | |
| V7: Service Registration Poisoning. | CVE-2021-21342 | unauthorized access identified in 2021 | CVE-2018-8037 | improper access control identified in 2018 | | |
| | CVE-2021-43980 | unauthorized access identified in 2021 | | | | |
| V8: Unauthorized Access to Service Discovery. | CVE-2023-46120 | unauthorized access identified in 2023 | CVE-2018-11784 | unauthorized access identified in 2018 | | |
| | CVE-2018-25031 | improper access control identified in 2018 | | | | |
| V9: Unavailability of Service Registration Validation. | | | | | CVE-2020-36186 | data leak vulnerability identified in 2020 |
| | | | | | CVE-2020-9488 | information disclosure identified in 2020 |
| V10: Unauthorized Service Deregistration. | CVE-2022-25647 | unauthorized access identified in 2022 | CVE-2023-41080 | improper access control identified in 2023 | | |
| | CVE-2022-40150 | improper access control identified in 2022 | | | | |
| | CVE-2021-46708 | improper access control identified in 2021 | | | | |
| V11: Reuse of Previous Service Requests. | | | | | | |
| V12: Legitimate Service Spoofing. | | | | | CVE-2019-17531 | information disclosure identified in 2019 |
| V13: Insufficient Network Segmentation. | CVE-2020-36183 | data leak vulnerability identified in 2020 | | | CVE-2023-38493 | improper access control identified in 2023 |
| V14: Improper Service Mesh Implementation. | CVE-2020-36185 | privilege escalation identified in 2020 | | | CVE-2020-9546 | unauthorized access identified in 2020 |
| | | | | | CVE-2019-12086 | unauthorized access identified in 2019 |
| V15: Misconfigured Network Access Controls. | | | | | | |
| V16: Incorrect Firewall Configuration. | | | | | CVE-2020-14195 | unauthorized access identified in 2020 |
| | | | | | CVE-2020-36189 | improper access control identified in 2020 |
| V17: No Internet Traffic Encryption. | | | | | CVE-2020-9548 | improper access control identified in 2020 |
| | | | | | CVE-2022-25857 | improper access control identified in 2022 |
| V18: Using Default Network Configurations. | | | | | | |
| V19: Using Weak or Deprecated Algorithms. | | | | | CVE-2019-16942 | buffer overflow identified in 2019 |
| | | | | | CVE-2020-14060 | buffer overflow identified in 2020 |
| V20: Lack of End-to-End Encryption. | | | | | CVE-2019-14892 | denial of service identified in 2019 |
| 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-2018-7489 | denial of service identified in 2018 | | | CVE-2022-42004 | denial of service identified in 2022 |
| | CVE-2020-36518 | denial of service identified in 2020 | | | CVE-2020-5398 | denial of service identified in 2020 |
| | CVE-2022-21363 | denial of service identified in 2022 | | | | |
| V26: Improper Handling of Suspicious. | CVE-2023-42795 | denial of service identified in 2023 | CVE-2022-42003 | denial of service identified in 2022 | CVE-2020-14062 | denial of service identified in 2020 |
| | | | CVE-2019-0199 | denial of service identified in 2019 | CVE-2019-12384 | denial of service identified in 2019 |
| V27: Lack of Individualized Rate Limiting. | CVE-2021-21344 | denial of service identified in 2021 | CVE-2020-11619 | denial of service identified in 2020 | CVE-2020-35491 | denial of service identified in 2020 |
| | | | CVE-2020-36187 | denial of service identified in 2020 | CVE-2019-9512 | denial of service identified in 2019 |
| | | | CVE-2019-17563 | denial of service identified in 2019 | CVE-2023-43642 | denial of service identified in 2023 |
| | | | CVE-2021-25329 | denial of service identified in 2021 | CVE-2023-20883 | denial of service identified in 2023 |
| V28: Improper Configuration of Rate Limits. | CVE-2020-14062 | denial of service identified in 2020 | | | CVE-2021-37136 | denial of service identified in 2021 |
| | | | | | CVE-2019-9515 | denial of service identified in 2019 |
| V29: Targeted API Abuse. | CVE-2021-42392 | denial of service identified in 2021 | | | CVE-2020-36185 | denial of service identified in 2020 |
| | | | | | CVE-2022-22965 | denial of service identified in 2022 |
| | | | | | CVE-2023-20863 | denial of service identified in 2023 |
| | | | | | CVE-2020-11022 | denial of service identified in 2020 |
| V30: Weak or Non-existent Database Encryption. | CVE-2021-21351 | information disclosure identified in 2021 | CVE-2019-14439 | information disclosure identified in 2019 | CVE-2021-22060 | information disclosure identified in 2021 |
| | CVE-2019-14900 | information disclosure identified in 2019 | CVE-2019-12814 | data leak vulnerability identified in 2019 | | |
| | CVE-2021-22118 | information disclosure identified in 2021 | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| V31: Inadequate Database Hardening. | CVE-2018-8014 | information disclosure identified in 2018 | CVE-2022-42004 | information disclosure identified in 2022 | CVE-2022-22950 | information disclosure identified in 2022 |
| | CVE-2020-8840 | data leak vulnerability identified in 2020 | CVE-2023-34036 | information disclosure identified in 2023 | | |
| | CVE-2020-11996 | information disclosure identified in 2020 | | | | |
| | CVE-2019-14379 | data leak vulnerability identified in 2019 | | | | |
| | CVE-2019-14339 | data leak vulnerability identified in 2019 | | | | |
| | CVE-2021-39149 | injection vulnerability identified in 2021 | | | | |
| | CVE-2021-43859 | data leak vulnerability identified in 2021 | | | | |
| | CVE-2021-28170 | data leak vulnerability identified in 2021 | | | | |
| | CVE-2021-30639 | data leak vulnerability identified in 2021 | | | | |
| | CVE-2023-24998 | data leak vulnerability identified in 2023 | | | | |
| V32: Using Default Database Credentials. | CVE-2022-23221 | data leak vulnerability identified in 2022 | CVE-2020-9546 | information disclosure identified in 2020 | CVE-2020-11111 | information disclosure identified in 2020 |
| | CVE-2020-36188 | data leak vulnerability identified in 2020 | CVE-2020-24616 | information disclosure identified in 2020 | CVE-2020-24616 | information disclosure identified in 2020 |
| | CVE-2020-11113 | information disclosure identified in 2020 | CVE-2021-20190 | information disclosure identified in 2021 | CVE-2020-36181 | data leak vulnerability identified in 2020 |
| | CVE-2020-36187 | information disclosure identified in 2020 | CVE-2019-0221 | information disclosure identified in 2019 | CVE-2021-21290 | data leak vulnerability identified in 2021 |
| | CVE-2020-10672 | information disclosure identified in 2020 | CVE-2022-22965 | information disclosure identified in 2022 | CVE-2022-38751 | information disclosure identified in 2022 |
| | CVE-2019-20330 | information disclosure identified in 2019 | CVE-2022-22950 | data leak vulnerability identified in 2022 | CVE-2020-5421 | information disclosure identified in 2020 |
| | CVE-2018-1000873 | information disclosure identified in 2018 | CVE-2022-38749 | information disclosure identified in 2022 | | |
| | CVE-2022-25857 | information disclosure identified in 2022 | | | | |
| | CVE-2020-26217 | data leak vulnerability identified in 2020 | | | | |
| | CVE-2021-23463 | data leak vulnerability identified in 2021 | | | | |
| | CVE-2022-45685 | data leak vulnerability identified in 2022 | | | | |
| | CVE-2018-1271 | data leak vulnerability identified in 2018 | | | | |
| | CVE-2023-20863 | information disclosure identified in 2023 | | | | |
| | CVE-2023-28708 | information disclosure identified in 2023 | | | | |
| | CVE-2021-30640 | data leak vulnerability identified in 2021 | | | | |
| | CVE-2021-22097 | data leak vulnerability identified in 2021 | | | | |
| | CVE-2018-15756 | information disclosure identified in 2018 | | | | |
| V33: Exposure of Sensitive Data via Error Messages. | CVE-2018-12023 | data leak vulnerability identified in 2018 | | | | |
| | CVE-2019-0199 | data leak vulnerability identified in 2019 | | | | |
| | CVE-2020-17527 | information disclosure identified in 2020 | | | | |
| | CVE-2022-38751 | information disclosure identified in 2022 | | | | |
| V34: Non-existent Data Integrity Checks. | CVE-2018-1273 | data leak vulnerability identified in 2018 | | | CVE-2020-8840 | data leak vulnerability identified in 2020 |
| | CVE-2020-5398 | information disclosure identified in 2020 | | | | |
| | CVE-2018-19361 | information disclosure identified in 2018 | | | | |
| | CVE-2020-35491 | information disclosure identified in 2020 | | | | |
| | CVE-2022-28749 | information disclosure identified in 2022 | | | | |
| V35: SQL Injection. | | | CVE-2020-36184 | remote code execution identified in 2020 | | |
| V36: Cross-Site Scripting (XSS). | CVE-2022-22963 | cross-site scripting (XSS) identified in 2022 | CVE-2018-14721 | cross-site scripting (XSS) identified in 2018 | CVE-2020-36184 | cross-site scripting (XSS) identified in 2020 |
| | CVE-2020-9547 | cross-site scripting (XSS) identified in 2020 | CVE-2019-14379 | cross-site scripting (XSS) identified in 2019 | CVE-2020-36188 | cross-site scripting (XSS) identified in 2020 |
| | CVE-2020-24750 | cross-site scripting (XSS) identified in 2020 | CVE-2018-12022 | cross-site scripting (XSS) identified in 2018 | CVE-2022-38752 | cross-site scripting (XSS) identified in 2022 |
| | CVE-2020-36186 | cross-site scripting (XSS) identified in 2020 | CVE-2020-11113 | cross-site scripting (XSS) identified in 2020 | CVE-2023-34454 | cross-site scripting (XSS) identified in 2023 |
| | CVE-2018-14718 | cross-site scripting (XSS) identified in 2018 | CVE-2020-11620 | cross-site scripting (XSS) identified in 2020 | CVE-2022-24785 | cross-site scripting (XSS) identified in 2022 |
| | CVE-2020-11620 | cross-site scripting (XSS) identified in 2020 | CVE-2020-14060 | cross-site scripting (XSS) identified in 2020 | CVE-2015-2575 | cross-site scripting (XSS) identified in 2015 |
| | CVE-2020-11619 | cross-site scripting (XSS) identified in 2020 | CVE-2020-14061 | cross-site scripting (XSS) identified in 2020 | | |
| | CVE-2019-17267 | cross-site scripting (XSS) identified in 2019 | CVE-2020-36179 | cross-site scripting (XSS) identified in 2020 | | |
| | CVE-2018-1336 | cross-site scripting (XSS) identified in 2018 | CVE-2020-36181 | cross-site scripting (XSS) identified in 2020 | | |
| | CVE-2023-20883 | cross-site scripting (XSS) identified in 2023 | CVE-2020-36183 | cross-site scripting (XSS) identified in 2020 | | |
| | CVE-2021-39150 | cross-site scripting (XSS) identified in 2021 | CVE-2020-1935 | cross-site scripting (XSS) identified in 2020 | | |
| | CVE-2021-21341 | cross-site scripting (XSS) identified in 2021 | CVE-2023-20861 | cross-site scripting (XSS) identified in 2023 | | |
| | CVE-2023-34050 | cross-site scripting (XSS) identified in 2023 | CVE-2022-21363 | cross-site scripting (XSS) identified in 2022 | | |
| | CVE-2022-45143 | cross-site scripting (XSS) identified in 2022 | CVE-2022-38750 | cross-site scripting (XSS) identified in 2022 | | |
| | CVE-2019-12814 | cross-site scripting (XSS) identified in 2019 | CVE-2023-1370 | cross-site scripting (XSS) identified in 2023 | | |
| | CVE-2021-25122 | cross-site scripting (XSS) identified in 2021 | | | | |
| | CVE-2023-45648 | cross-site scripting (XSS) identified in 2023 | | | | |
| | CVE-2020-13956 | cross-site scripting (XSS) identified in 2020 | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | CVE-2022-22968 | cross-site scripting (XSS) identified in 2022 | | | | |
| | CVE-2019-3797 | cross-site scripting (XSS) identified in 2019 | | | | |
| | CVE-2022-38750 | cross-site scripting (XSS) identified in 2022 | | | | |
| V37: Command Injection. | CVE-2018-14721 | buffer overflow identified in 2018 | CVE-2018-12023 | buffer overflow identified in 2018 | CVE-2019-14540 | cross-site scripting (XSS) identified in 2019 |
| | CVE-2020-14195 | buffer overflow identified in 2020 | CVE-2018-19362 | buffer overflow identified in 2018 | CVE-2021-38153 | buffer overflow identified in 2021 |
| | CVE-2019-16942 | buffer overflow identified in 2019 | CVE-2020-11111 | buffer overflow identified in 2020 | CVE-2023-34462 | buffer overflow identified in 2023 |
| | CVE-2021-20190 | buffer overflow identified in 2021 | CVE-2020-36189 | buffer overflow identified in 2020 | CVE-2022-38749 | buffer overflow identified in 2022 |
| | CVE-2021-39144 | buffer overflow identified in 2021 | CVE-2019-10072 | buffer overflow identified in 2019 | CVE-2023-34453 | buffer overflow identified in 2023 |
| | CVE-2021-39147 | buffer overflow identified in 2021 | CVE-2022-22970 | buffer overflow identified in 2022 | CVE-2022-22970 | buffer overflow identified in 2022 |
| | CVE-2021-39152 | buffer overflow identified in 2021 | CVE-2023-20863 | buffer overflow identified in 2023 | CVE-2010-1621 | buffer overflow identified in 2010 |
| | CVE-2021-21346 | buffer overflow identified in 2021 | CVE-2023-20873 | buffer overflow identified in 2023 | CVE-2007-2691 | buffer overflow identified in 2007 |
| | CVE-2021-21348 | buffer overflow identified in 2021 | | | CVE-2019-11358 | buffer overflow identified in 2019 |
| | CVE-2022-22979 | buffer overflow identified in 2022 | | | CVE-2020-11023 | buffer overflow identified in 2020 |
| | CVE-2022-40152 | buffer overflow identified in 2022 | | | | |
| | CVE-2022-45868 | buffer overflow identified in 2022 | | | | |
| | CVE-2022-40160 | buffer overflow identified in 2022 | | | | |
| | CVE-2021-2471 | buffer overflow identified in 2021 | | | | |
| V38: Insecure Deserialization of Data. | | | CVE-2020-36185 | remote code execution identified in 2020 | | |
| V39: User Inputs Directly Accessing Objects. | CVE-2018-14719 | buffer overflow identified in 2018 | | | CVE-2020-8908 | cross-site scripting (XSS) identified in 2020 |
| | | | | | CVE-2022-41915 | buffer overflow identified in 2022 |
| | | | | | CVE-2009-0819 | buffer overflow identified in 2009 |
| V40: Granting Higher than Required Level of Access. | CVE-2019-12384 | privilege escalation identified in 2019 | CVE-2019-14893 | privilege escalation identified in 2019 | | |
| | CVE-2020-9548 | privilege escalation identified in 2020 | CVE-2021-23463 | privilege escalation identified in 2021 | | |
| | CVE-2023-1370 | privilege escalation identified in 2023 | | | | |
| | CVE-2021-39140 | privilege escalation identified in 2021 | | | | |
| V41: Credential Hardcoding in Source Code. | | | | | | |
| V42: Granted Privilege Exploitation. | CVE-2021-22096 | privilege escalation identified in 2021 | CVE-2020-9548 | privilege escalation identified in 2020 | | |
| | | | CVE-2022-38752 | privilege escalation identified in 2022 | | |
| V43: Race Condition Exploitation. | | | | | | |
| V44: Improper Data Transaction Management. | CVE-2020-25649 | information disclosure identified in 2020 | | | | |
| V45: Insecure Data Synchronization. | CVE-2020-10968 | information disclosure identified in 2020 | CVE-2022-22968 | data leak vulnerability identified in 2022 | | |
| | CVE-2021-39151 | information disclosure identified in 2021 | | | | |
| | CVE-2018-11784 | data leak vulnerability identified in 2018 | | | | |
| | CVE-2021-22047 | information disclosure identified in 2021 | | | | |
| V46: Concurrent Data Access Mismanagement. | | | CVE-2019-12418 | information disclosure identified in 2019 | CVE-2023-34455 | data leak vulnerability identified in 2023 |
| V47: Lack of Regular Backups. | CVE-2019-12086 | data leak vulnerability identified in 2019 | CVE-2019-16943 | data leak vulnerability identified in 2019 | | |
| | CVE-2022-38749 | information disclosure identified in 2022 | CVE-2020-1938 | information disclosure identified in 2020 | | |
| | CVE-2022-40159 | information disclosure identified in 2022 | CVE-2018-15756 | data leak vulnerability identified in 2018 | | |
| | CVE-2019-0221 | information disclosure identified in 2019 | | | | |
| V48: Insecure Backup Storage. | CVE-2021-39154 | information disclosure identified in 2021 | | | | |
| V49: Lack of Backup Validation. | CVE-2020-24616 | data leak vulnerability identified in 2020 | CVE-2020-10968 | data leak vulnerability identified in 2020 | | |
| | CVE-2020-9546 | information disclosure identified in 2020 | CVE-2018-1272 | information disclosure identified in 2018 | | |
| | CVE-2021-39153 | data leak vulnerability identified in 2021 | | | | |
| V50: Improper Disposal of Outdated Backups. | | | CVE-2018-1271 | information disclosure identified in 2018 | CVE-2020-10672 | information disclosure identified in 2020 |
| V51: Insecure/Weak Authentication. | CVE-2019-14893 | unauthorized access identified in 2019 | CVE-2020-10673 | improper access control identified in 2020 | CVE-2022-41854 | improper access control identified in 2022 |
| | CVE-2021-39146 | improper access control identified in 2021 | | | | |
| V52: Enumeration of Accounts. | CVE-2022-42003 | unauthorized access identified in 2022 | | | | |
| V53: Continued Usage of Breached Credentials. | CVE-2020-36189 | privilege escalation identified in 2020 | | | | |
| | CVE-2021-25329 | improper access control identified in 2021 | | | | |
| V54: Identity Federation Misconfiguration. | CVE-2021-24122 | improper access control identified in 2021 | | | | |
| V55: Provision of Higher Privileges. | CVE-2022-22965 | privilege escalation identified in 2022 | CVE-2018-7489 | privilege escalation identified in 2018 | | |
| | CVE-2020-36184 | privilege escalation identified in 2020 | CVE-2019-12086 | privilege escalation identified in 2019 | | |
| | CVE-2020-10650 | privilege escalation identified in 2020 | CVE-2020-36182 | privilege escalation identified in 2020 | | |
| | CVE-2018-10054 | privilege escalation identified in 2018 | CVE-2019-10219 | privilege escalation identified in 2019 | | |
| | CVE-2023-1436 | privilege escalation identified in 2023 | CVE-2023-20883 | privilege escalation identified in 2023 | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | CVE-2023-4759 | privilege escalation identified in 2023 | CVE-2022-1471 | privilege escalation identified in 2022 | | |
| | CVE-2017-18640 | privilege escalation identified in 2017 | CVE-2022-23221 | privilege escalation identified in 2022 | | |
| | CVE-2018-11039 | privilege escalation identified in 2018 | | | | |
| | CVE-2019-3802 | privilege escalation identified in 2019 | | | | |
| | CVE-2022-31679 | privilege escalation identified in 2022 | | | | |
| V56: Improper Token Invalidation. | | | CVE-2020-36188 | unauthorized access identified in 2020 | | |
| V57: Insecure Access Token Storage. | CVE-2020-36180 | unauthorized access identified in 2020 | CVE-2020-10672 | improper access control identified in 2020 | | |
| | CVE-2020-26259 | data leak vulnerability identified in 2020 | | | | |
| V58: Embedded Static Credentials. | CVE-2020-36179 | unauthorized access identified in 2020 | CVE-2020-36518 | improper access control identified in 2020 | CVE-2022-31129 | improper access control identified in 2022 |
| | CVE-2023-34036 | improper access control identified in 2023 | | | | |
| V59: Reuse of Passwords. | CVE-2020-36181 | unauthorized access identified in 2020 | CVE-2019-17531 | unauthorized access identified in 2019 | | |
| | CVE-2018-12022 | unauthorized access identified in 2018 | CVE-2020-36180 | improper access control identified in 2020 | | |
| | CVE-2022-40151 | improper access control identified in 2022 | CVE-2022-38751 | improper access control identified in 2022 | | |
| V60: Vulnerable Password Recovery Process. | CVE-2021-33037 | improper access control identified in 2021 | CVE-2020-14062 | improper access control identified in 2020 | | |
| V61: MFA not Used/Enforced. | CVE-2022-22970 | unauthorized access identified in 2022 | CVE-2020-14195 | unauthorized access identified in 2020 | | |
| | CVE-2023-20861 | unauthorized access identified in 2023 | | | | |
| V62: Phishing Attacks on Users. | CVE-2019-16943 | unauthorized access identified in 2019 | CVE-2019-17267 | improper access control identified in 2019 | CVE-2009-4028 | unauthorized access identified in 2009 |
| V63: Unenforced Access Controls. | CVE-2020-5421 | privilege escalation identified in 2020 | | | | |
| | CVE-2022-1471 | privilege escalation identified in 2022 | | | | |
| | CVE-2021-21343 | privilege escalation identified in 2021 | | | | |
| V64: Human Error in Granting Access. | CVE-2020-25638 | improper access control identified in 2020 | CVE-2022-45868 | unauthorized access identified in 2022 | CVE-2007-5925 | unauthorized access identified in 2007 |
| V65: Insecure Direct Object Reference. | CVE-2019-14540 | remote code execution identified in 2019 | CVE-2019-20330 | remote code execution identified in 2019 | CVE-2020-10673 | remote code execution identified in 2020 |
| | CVE-2018-14720 | remote code execution identified in 2018 | CVE-2020-25649 | remote code execution identified in 2020 | CVE-2020-10968 | remote code execution identified in 2020 |
| | CVE-2020-14060 | remote code execution identified in 2020 | CVE-2019-12384 | remote code execution identified in 2019 | CVE-2020-36187 | remote code execution identified in 2020 |
| | CVE-2019-17531 | remote code execution identified in 2019 | CVE-2022-22971 | remote code execution identified in 2022 | CVE-2021-21295 | remote code execution identified in 2021 |
| | CVE-2018-1274 | improper access control identified in 2018 | CVE-2021-42392 | remote code execution identified in 2021 | | |
| | CVE-2021-39145 | remote code execution identified in 2021 | | | | |
| | CVE-2018-8037 | remote code execution identified in 2018 | | | | |
| | CVE-2021-46877 | remote code execution identified in 2021 | | | | |
| | CVE-2022-42252 | remote code execution identified in 2022 | | | | |
| V66: Vulnerable APIs Having Higher Control. | CVE-2019-0232 | improper access control identified in 2019 | CVE-2019-16942 | improper access control identified in 2019 | | |
| | CVE-2022-27772 | unauthorized access identified in 2022 | | | | |
| | CVE-2018-1272 | unauthorized access identified in 2018 | | | | |
| | CVE-2020-26258 | improper access control identified in 2020 | | | | |
| V67: Session Hijacking. | CVE-2020-9484 | unauthorized access identified in 2020 | | | CVE-2019-8331 | improper access control identified in 2019 |
| | CVE-2018-1000632 | improper access control identified in 2018 | | | | |
| | CVE-2019-16335 | unauthorized access identified in 2019 | | | | |
| | CVE-2021-22060 | unauthorized access identified in 2021 | | | | |
| V68: Cross-Site Request Forgery. | CVE-2021-41079 | unauthorized access identified in 2021 | CVE-2018-14720 | improper access control identified in 2018 | | |
| | CVE-2022-23181 | improper access control identified in 2022 | CVE-2019-3797 | unauthorized access identified in 2019 | | |
| | | | CVE-2019-3802 | unauthorized access identified in 2019 | | |
| V69: Session Control Exploitation. | CVE-2020-35728 | unauthorized access identified in 2020 | CVE-2018-14719 | improper access control identified in 2018 | CVE-2016-1000027 | unauthorized access identified in 2016 |
| | CVE-2019-10072 | improper access control identified in 2019 | CVE-2019-14892 | unauthorized access identified in 2019 | | |
| | CVE-2020-13943 | unauthorized access identified in 2020 | CVE-2021-22060 | unauthorized access identified in 2021 | | |
| | CVE-2020-15522 | unauthorized access identified in 2020 | CVE-2021-22047 | improper access control identified in 2021 | | |
| V70: Improper Session Expiry. | CVE-2020-14061 | improper access control identified in 2020 | CVE-2020-36186 | unauthorized access identified in 2020 | CVE-2022-22968 | improper access control identified in 2022 |
| | CVE-2021-39141 | improper access control identified in 2021 | CVE-2020-10693 | unauthorized access identified in 2020 | | |
| | | | CVE-2022-41854 | unauthorized access identified in 2022 | | |
| V71: Container Misconfigurations. | | | | | CVE-2019-16335 | remote code execution identified in 2019 |
| V72: Improper Container Isolation. | | | | | CVE-2020-24750 | privilege escalation identified in 2020 |
| V73: Direct Storage of Sensitive Data on Container Image. | CVE-2020-8908 | information disclosure identified in 2020 | | | CVE-2010-1626 | remote code execution identified in 2010 |
| V74: Outdated/Insecure Container Image Usage. | | | | | CVE-2023-2976 | buffer overflow identified in 2023 |
| | | | | | CVE-2020-35490 | privilege escalation identified in 2020 |
| | | | | | CVE-2023-20861 | privilege escalation identified in 2023 |
| V75: Misconfiguration of Orchestration Dashboards. | | | | | CVE-2019-17267 | privilege escalation identified in 2019 |

|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
| V76: Orchestration Tools Having Unrestricted API Access. |  |  |  |  |  |  |
| V77: Poor Definition of RBAC. | CVE-2019-14892 | privilege escalation identified in 2019 | CVE-2021-42550 | privilege escalation identified in 2021 |  |  |
|  | CVE-2021-21350 | privilege escalation identified in 2021 |  |  |  |  |
|  | CVE-2022-22976 | privilege escalation identified in 2022 |  |  |  |  |
|  | CVE-2021-22113 | privilege escalation identified in 2021 |  |  |  |  |
| V78: Vulnerabilities in Orchestration Tools. | CVE-2023-20873 | remote code execution identified in 2023 |  |  | CVE-2020-5397 | privilege escalation identified in 2020 |
| V79: Insecure Service Configuration. |  |  |  |  |  |  |
| V80: Service Deployments with no Configuration Validation. |  |  |  |  |  |  |
| V81: Embedded Passwords/Tokens in Configuration Files. | CVE-2019-17563 | unauthorized access identified in 2019 | CVE-2018-11040 | improper access control identified in 2018 |  |  |
| V82: Insecure Configuration File Validation. | CVE-2023-41080 | remote code execution identified in 2023 | CVE-2019-14540 | remote code execution identified in 2019 | CVE-2021-0341 | remote code execution identified in 2021 |
|  |  |  | CVE-2020-9547 | remote code execution identified in 2020 | CVE-2010-3677 | remote code execution identified in 2010 |
|  |  |  | CVE-2020-10650 | remote code execution identified in 2020 |  |  |
|  |  |  | CVE-2019-0232 | remote code execution identified in 2019 |  |  |
| V83: Adding Components with Known Vulnerabilities. | CVE-2020-36182 | remote code execution identified in 2020 | CVE-2018-1000873 | remote code execution identified in 2018 |  |  |
|  | CVE-2023-2976 | improper access control identified in 2023 | CVE-2021-24122 | remote code execution identified in 2021 |  |  |
|  |  |  | CVE-2016-1000027 | remote code execution identified in 2016 |  |  |
| V84: Outdated/Unmaintained Dependency Usage. |  |  | CVE-2018-11039 | remote code execution identified in 2018 | CVE-2019-14893 | remote code execution identified in 2019 |
|  |  |  |  |  | CVE-2021-20190 | remote code execution identified in 2021 |
|  |  |  |  |  | CVE-2022-24823 | remote code execution identified in 2022 |
| V85: Insufficient Scanning of Dependencies. |  |  |  |  |  |  |
| V86: No Transitive Dependency Validation. | CVE-2023-33201 | privilege escalation identified in 2023 | CVE-2018-14718 | privilege escalation identified in 2018 |  |  |
|  | CVE-2022-40149 | privilege escalation identified in 2022 | CVE-2020-8840 | privilege escalation identified in 2020 |  |  |
|  | CVE-2022-38752 | privilege escalation identified in 2022 | CVE-2018-8034 | privilege escalation identified in 2018 |  |  |
|  |  |  | CVE-2018-1257 | privilege escalation identified in 2018 |  |  |
|  |  |  | CVE-2021-2471 | privilege escalation identified in 2021 |  |  |
| V87: Inconsistent Security Practices. |  |  |  |  | CVE-2020-13946 | buffer overflow identified in 2020 |
| V88: Issues Within Specific Libraries. |  |  |  |  | CVE-2017-18640 | remote code execution identified in 2017 |
| V89: Misconfiguration of Different Platforms. |  |  |  |  | CVE-2022-1471 | unauthorized access identified in 2022 |
| V90: Patch Management Complexity. |  |  |  |  | CVE-2019-20444 | improper access control identified in 2019 |
| V91: Legacy System Integration Vulnerabilities. |  |  |  |  | CVE-2020-36182 | improper access control identified in 2020 |
| V92: Mismatched Data Formats in Different Technologies. |  |  |  |  |  |  |
| V93: Service Mesh Configuration Errors. |  |  |  |  |  |  |
| V94: Inconsistent Security at Integration Points. | CVE-2020-10673 | denial of service identified in 2020 | CVE-2019-16335 | denial of service identified in 2019 |  |  |
|  | CVE-2018-11307 | denial of service identified in 2018 | CVE-2020-35490 | denial of service identified in 2020 |  |  |
|  | CVE-2020-10683 | denial of service identified in 2020 | CVE-2018-1336 | denial of service identified in 2018 |  |  |
|  | CVE-2022-22950 | denial of service identified in 2022 | CVE-2021-46877 | denial of service identified in 2021 |  |  |
| V95: Compromised Supply Chain Attacks. |  |  |  |  | CVE-2019-14439 | data leak vulnerability identified in 2019 |
| V96: Third-Party Components Service Outages. | CVE-2019-10219 | denial of service identified in 2019 | CVE-2018-19361 | denial of service identified in 2018 |  |  |
|  | CVE-2020-13934 | denial of service identified in 2020 | CVE-2021-22096 | denial of service identified in 2021 |  |  |
|  | CVE-2021-22095 | denial of service identified in 2021 |  |  |  |  |
| V97: Insecure Third-Party Components. |  |  | CVE-2018-11307 | unauthorized access identified in 2018 |  |  |
|  |  |  | CVE-2018-8014 | improper access control identified in 2018 |  |  |
|  |  |  | CVE-2018-1270 | improper access control identified in 2018 |  |  |
| V98: No Proper Security Practices in Third-Party Components. |  |  |  |  | CVE-2020-11112 | remote code execution identified in 2020 |
| V99: Various Injection Vulnerabilities. | CVE-2023-20860 | injection vulnerability identified in 2023 | CVE-2018-19360 | injection vulnerability identified in 2018 | CVE-2023-44487 | injection vulnerability identified in 2023 |
|  | CVE-2018-19360 | injection vulnerability identified in 2018 | CVE-2020-10969 | injection vulnerability identified in 2020 | CVE-2018-1000873 | injection vulnerability identified in 2018 |
|  | CVE-2020-11111 | injection vulnerability identified in 2020 | CVE-2020-11112 | injection vulnerability identified in 2020 | CVE-2019-16943 | injection vulnerability identified in 2019 |
|  | CVE-2020-11112 | injection vulnerability identified in 2020 | CVE-2020-24750 | injection vulnerability identified in 2020 | CVE-2020-11620 | injection vulnerability identified in 2020 |
|  | CVE-2020-35490 | injection vulnerability identified in 2020 | CVE-2020-35491 | injection vulnerability identified in 2020 | CVE-2020-35728 | injection vulnerability identified in 2020 |
|  | CVE-2021-39148 | injection vulnerability identified in 2021 | CVE-2021-25122 | injection vulnerability identified in 2021 | CVE-2020-11612 | injection vulnerability identified in 2020 |
|  | CVE-2022-45693 | injection vulnerability identified in 2022 | CVE-2020-25638 | injection vulnerability identified in 2020 | CVE-2022-41881 | injection vulnerability identified in 2022 |
|  | CVE-2022-42004 | injection vulnerability identified in 2022 | CVE-2022-27772 | injection vulnerability identified in 2022 | CVE-2023-4586 | injection vulnerability identified in 2023 |
|  | CVE-2018-11040 | injection vulnerability identified in 2018 | CVE-2018-1275 | injection vulnerability identified in 2018 | CVE-2021-43797 | injection vulnerability identified in 2021 |
|  | CVE-2020-10693 | injection vulnerability identified in 2020 | CVE-2020-5398 | injection vulnerability identified in 2020 | CVE-2021-21409 | injection vulnerability identified in 2021 |
|  | CVE-2021-29505 | injection vulnerability identified in 2021 | CVE-2021-22118 | injection vulnerability identified in 2021 | CVE-2019-9514 | injection vulnerability identified in 2019 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | CVE-2022-41966 | injection vulnerability identified in 2022 | CVE-2022-25857 | injection vulnerability identified in 2022 | CVE-2021-22118 | injection vulnerability identified in 2021 |
| | CVE-2021-21345 | injection vulnerability identified in 2021 | | | CVE-2021-22096 | injection vulnerability identified in 2021 |
| | CVE-2021-29425 | injection vulnerability identified in 2021 | | | CVE-2007-1420 | injection vulnerability identified in 2007 |
| | CVE-2018-14335 | injection vulnerability identified in 2018 | | | CVE-2020-23064 | injection vulnerability identified in 2020 |
| | CVE-2022-41854 | injection vulnerability identified in 2022 | | | | |
| V100: Improper XSS Prevention Implementation. | | | | | CVE-2023-46120 | cross-site scripting (XSS) identified in 2023 |
| | | | | | CVE-2018-10237 | cross-site scripting (XSS) identified in 2018 |
| | | | | | CVE-2020-10969 | cross-site scripting (XSS) identified in 2020 |
| | | | | | CVE-2020-10650 | cross-site scripting (XSS) identified in 2020 |
| | | | | | CVE-2020-36179 | cross-site scripting (XSS) identified in 2020 |
| | | | | | CVE-2020-36183 | cross-site scripting (XSS) identified in 2020 |
| | | | | | CVE-2020-25649 | cross-site scripting (XSS) identified in 2020 |
| | | | | | CVE-2021-37714 | cross-site scripting (XSS) identified in 2021 |
| | | | | | CVE-2019-12399 | cross-site scripting (XSS) identified in 2019 |
| | | | | | CVE-2019-16869 | cross-site scripting (XSS) identified in 2019 |
| | | | | | CVE-2021-37137 | cross-site scripting (XSS) identified in 2021 |
| | | | | | CVE-2019-9518 | cross-site scripting (XSS) identified in 2019 |
| | | | | | CVE-2017-15945 | cross-site scripting (XSS) identified in 2017 |
| | | | | | CVE-2010-3682 | cross-site scripting (XSS) identified in 2010 |
| V101: Insecure Deserialization in components. | | | | | | |
| V102: Flaws in Specific Frameworks. | | | | | CVE-2020-11113 | remote code execution identified in 2020 |
| | | | | | CVE-2022-38750 | improper access control identified in 2022 |
| V103: Cloud Environment Misconfiguration. | | | | | CVE-2023-35116 | privilege escalation identified in 2023 |
| V104: Infrastructure Tools Misconfiguration. | | | | | CVE-2019-20445 | privilege escalation identified in 2019 |
| V105: Mismanagement of VMs. | | | | | CVE-2020-11619 | privilege escalation identified in 2020 |
| V106: Insufficient Network Security. | | | | | CVE-2020-36518 | remote code execution identified in 2020 |
| | | | | | CVE-2022-27772 | improper access control identified in 2022 |
| V107: Lack of Integration Tool Security. | | | | | CVE-2021-44832 | information disclosure identified in 2021 |
| V108: CI/CD Misconfigurations. | | | | | CVE-2020-9547 | privilege escalation identified in 2020 |
| V109: Pipeline not having Security Controls. | | | | | CVE-2021-45105 | information disclosure identified in 2021 |
| V110: Vulnerable Code Deployment. | | | | | CVE-2022-36033 | unauthorized access identified in 2022 |
| V111: Insecure IaC Scripts. | | | | | CVE-2022-42003 | unauthorized access identified in 2022 |
| V112: Automated Deployment of Misconfigured Infrastructure. | | | | | CVE-2019-14379 | remote code execution identified in 2019 |
| | | | | | CVE-2020-14061 | privilege escalation identified in 2020 |
| V113: Secrets Hardcoded Within IaC Scripts. | CVE-2022-22971 | data leak vulnerability identified in 2022 | | | | |
| V114: No Version Control for IaC. | | | | | CVE-2023-3635 | improper access control identified in 2023 |
| V115: Insufficient Storage and Rotation of Secrets. | | | | | CVE-2023-0833 | unauthorized access identified in 2023 |
| V116: No Centralized Secrets Management System. | | | | | CVE-2018-17196 | data leak vulnerability identified in 2018 |
| V117: Committing Secrets in Version Control. | CVE-2021-21347 | data leak vulnerability identified in 2021 | | | | |
| V118: Failure to Monitor Secrets Access Logs. | | | | | CVE-2023-25194 | data leak vulnerability identified in 2023 |
| | | | | | CVE-2023-20873 | unauthorized access identified in 2023 |
| V119: Not Having Enough Automated Testing. | | | | | CVE-2021-44228 | information disclosure identified in 2021 |
| V120: Poor/no Manual Reviews of Security. | | | | | CVE-2019-12814 | remote code execution identified in 2019 |
| V121: Not Acting on Test Results. | | | | | CVE-2020-36180 | remote code execution identified in 2020 |
| V122: Outdated Testing Tools Used. | | | | | CVE-2021-45046 | data leak vulnerability identified in 2021 |
| 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. | | | | | | |