

Snyk Report

Jaspersoft Studio Example created by Mathias Conradt & Sebastian Roth

Sunday 30 April 2023



| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|-----------------------------------|----------------------|---|------------------|------------------|----------------------------|------------------|
| Critical | 899 | Arbitrary File Write via Archive Extraction (Zip Slip) | ["CVE-2018-1002204"] | ["CWE-29"] | e-corp-demo/goof-kubernetes(master):package.json | Mature | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 820 | NoSQL Injection | [] | ["CWE-89"] | e-corp-demo/goof-kubernetes(master) | | Not Auto Fixable | 2023-03-07 23:04:24.374 | Snyk Code |
| High | 820 | NoSQL Injection | [] | ["CWE-89"] | e-corp-demo/goof-kubernetes(master) | | Not Auto Fixable | 2023-03-07 23:04:24.374 | Snyk Code |
| High | 820 | NoSQL Injection | [] | ["CWE-89"] | e-corp-demo/goof-kubernetes(master) | | Not Auto Fixable | 2023-03-07 23:04:24.374 | Snyk Code |
| High | 807 | Hardcoded Secret | [] | ["CWE-547"] | e-corp-demo/goof-kubernetes(master) | | Not Auto Fixable | 2023-03-07 23:04:24.374 | Snyk Code |
| Critical | 800 | Arbitrary Code Execution | ["CVE-2017-5638"] | ["CWE-94"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Mature | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Critical | 800 | Remote Code Execution (RCE) | ["CVE-2021-44228"] | ["CWE-94"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Mature | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Critical | 800 | Remote Code Execution (RCE) | ["CVE-2021-44228"] | ["CWE-94"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-client/pom.xml | Mature | Auto Fixable | 2023-03-07 21:11:10.235 | Snyk Open Source |
| Critical | 790 | Remote Code Execution | ["CVE-2022-22965"] | ["CWE-94"] | e-corp-demo/java-goof(main):todolist-goof/todolist-core/pom.xml | Mature | Auto Fixable | 2023-03-07 21:11:13.069 | Snyk Open Source |
| Critical | 790 | Deserialization of Untrusted Data | ["CVE-2015-7501","CVE-2015-4852"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | Mature | Not Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| Critical | 790 | Deserialization of Untrusted Data | ["CVE-2015-7501","CVE-2015-4852"] | ["CWE-502"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/pom.xml | Mature | Auto Fixable | 2023-03-07 21:11:12.255 | Snyk Open Source |
| Critical | 790 | Remote Code Execution (RCE) | ["CVE-2020-17530"] | ["CWE-94"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Mature | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Critical | 790 | Remote Code Execution | ["CVE-2022-22965"] | ["CWE-94"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Mature | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Critical | 790 | Arbitrary Command Execution | ["CVE-2016-3087"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Mature | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Critical | 760 | Remote Code Execution (RCE) | ["CVE-2019-0230"] | ["CWE-94"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Mature | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Critical | 760 | Deserialization of Untrusted Data | ["CVE-2017-5645"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Mature | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Critical | 760 | Arbitrary Code Execution | ["CVE-2017-12611"] | ["CWE-20","CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Mature | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 756 | Uninitialized Memory Exposure | [] | ["CWE-201"] | e-corp-demo/goof-kubernetes(master):package.json | Mature | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 751 | Prototype Pollution | ["CVE-2021-4264"] | ["CWE-1321"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 750 | Container is running without root user control | [] | [] | e-corp-demo/goof-kubernetes(master):goof-deployment.yaml | | Not Auto Fixable | 2023-03-07 23:04:06.635 | Snyk IaC |
| High | 750 | Container is running without root user control | [] | [] | e-corp-demo/goof-kubernetes(master):goof-mongo-deployment.yaml | | Not Auto Fixable | 2023-03-07 23:04:06.675 | Snyk IaC |
| High | 750 | Container is running without root user control | [] | [] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/k8s/deploy.yaml | | Not Auto Fixable | 2023-03-07 21:11:03.946 | Snyk IaC |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|---|----------------------|-----------------------|---|------------------|------------------|-------------------------|------------------|
| High | 750 | Container is running without privilege escalation control | | | e-corp-demo/goof-kubernetes(master):goof-mongo-deployment.yaml | | Not Auto Fixable | 2023-03-07 23:04:06.675 | Snyk IaC |
| High | 750 | Container is running without privilege escalation control | | | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/k8s/deploy.yaml | | Not Auto Fixable | 2023-03-07 21:11:03.946 | Snyk IaC |
| High | 750 | Container is running without privilege escalation control | | | e-corp-demo/goof-kubernetes(master):goof-deployment.yaml | | Not Auto Fixable | 2023-03-07 23:04:06.635 | Snyk IaC |
| High | 741 | DLL Injection | ["CVE-2020-13110"] | ["CWE-114"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 731 | Prototype Pollution | ["CVE-2020-8203"] | ["CWE-1321"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 726 | Remote Code Execution (RCE) | ["CVE-2022-29078"] | ["CWE-94"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Critical | 714 | Out-of-bounds Read | ["CVE-2019-19949"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Critical | 714 | Integer Overflow or Wraparound | ["CVE-2018-14618"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Critical | 714 | OS Command Injection | ["CVE-2017-17458"] | ["CWE-78"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Critical | 714 | Out-of-bounds Read | ["CVE-2017-8817"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Critical | 714 | Out-of-bounds Read | ["CVE-2018-16842"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Critical | 714 | Integer Overflow or Wraparound | ["CVE-2017-8816"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Critical | 714 | Out-of-bounds Read | ["CVE-2018-1000005"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Critical | 714 | Out-of-bounds Read | ["CVE-2018-1000122"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Critical | 714 | Double Free | ["CVE-2021-22945"] | ["CWE-415"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Critical | 714 | CVE-2018-1000007 | ["CVE-2018-1000007"] | | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Critical | 714 | OS Command Injection | ["CVE-2022-1292"] | ["CWE-78"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Critical | 714 | CVE-2019-9636 | ["CVE-2019-9636"] | | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Critical | 714 | OS Command Injection | ["CVE-2022-1292"] | ["CWE-78"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Critical | 714 | NULL Pointer Dereference | ["CVE-2017-14532"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Critical | 714 | Incorrect Default Permissions | ["CVE-2022-32207"] | ["CWE-276"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Critical | 714 | Out-of-Bounds | ["CVE-2017-1000257"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Critical | 714 | Out-of-bounds Read | ["CVE-2021-46848"] | ["CWE-125"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Critical | 714 | NULL Pointer Dereference | ["CVE-2017-14625"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Critical | 714 | Out-of-bounds Write | ["CVE-2018-14551"] | ["CWE-787","CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Critical | 714 | Out-of-bounds Write | ["CVE-2018-1000120"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Critical | 714 | Integer Overflow or Wraparound | ["CVE-2017-14062"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Critical | 714 | Buffer Overflow | ["CVE-2021-3177"] | ["CWE-120"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|---|----------------------|----------------------|--|------------------|--------------|-------------------------|------------------|
| Critical | 714 | Out-of-bounds Write | ["CVE-2019-5953"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Critical | 714 | Exposure of Resource to Wrong Sphere | ["CVE-2022-32221"] | ["CWE-668"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Critical | 714 | Buffer Overflow | ["CVE-2019-5482"] | ["CWE-120"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Critical | 714 | Buffer Overflow | ["CVE-2019-5482"] | ["CWE-120"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Critical | 714 | Double Free | ["CVE-2019-5481"] | ["CWE-415"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Critical | 714 | Double Free | ["CVE-2019-5481"] | ["CWE-415"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Critical | 714 | Out-of-bounds Read | ["CVE-2018-1000301"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Critical | 714 | Out-of-bounds Read | ["CVE-2017-8872"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Critical | 714 | Out-of-bounds Read | ["CVE-2017-8872"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Critical | 714 | Out-of-Bounds | ["CVE-2018-16839"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Critical | 714 | CVE-2019-9636 | ["CVE-2019-9636"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Critical | 714 | Directory Traversal | ["CVE-2022-1664"] | ["CWE-22"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Critical | 714 | Directory Traversal | ["CVE-2022-1664"] | ["CWE-22"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Critical | 714 | Buffer Overflow | ["CVE-2021-3177"] | ["CWE-120"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Critical | 714 | NULL Pointer Dereference | ["CVE-2017-18211"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Critical | 714 | Directory Traversal | ["CVE-2019-9948"] | ["CWE-22"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Critical | 714 | NULL Pointer Dereference | ["CVE-2017-14624"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Critical | 714 | Directory Traversal | ["CVE-2019-9948"] | ["CWE-22"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Critical | 714 | Out-of-bounds Write | ["CVE-2019-3822"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Critical | 714 | Integer Overflow or Wraparound | ["CVE-2022-41903"] | ["CWE-190"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Critical | 714 | NULL Pointer Dereference | ["CVE-2017-14626"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Critical | 714 | Integer Overflow or Wraparound | ["CVE-2022-23521"] | ["CWE-190"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Critical | 714 | Integer Overflow or Wraparound | ["CVE-2018-13347"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Critical | 714 | Credentials Management | ["CVE-2019-10160"] | ["CWE-255"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Critical | 714 | Incorrect Permission Assignment for Critical Resource | ["CVE-2018-1000132"] | ["CWE-732"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 711 | Cross-site Scripting (XSS) | ["CVE-2020-11022"] | ["CWE-79"] | e-corp-demo/goof-kubernetes(master):package.json | Mature | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 705 | Command Injection | ["CVE-2016-3081"] | ["CWE-77"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Mature | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 705 | Arbitrary Command Execution | ["CVE-2017-9805"] | ["CWE-20","CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Mature | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|------------------------------------|-----------------------|---|------------------|------------------|-------------------------|------------------|
| High | 705 | Remote Code Execution | ["CVE-2018-11776"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Mature | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 705 | Deserialization of Untrusted Data | ["CVE-2019-12384"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | Mature | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 705 | Command Injection | ["CVE-2016-3081"] | ["CWE-77"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Mature | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Medium | 701 | Cross-site Scripting (XSS) | ["CVE-2020-11023"] | ["CWE-79"] | e-corp-demo/goof-kubernetes(master):package.json | Mature | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 696 | Prototype Poisoning | ["CVE-2022-24999"] | ["CWE-1321"] | e-corp-demo/container-breaking-in-goof(main):package.json | Proof of Concept | Auto Fixable | 2023-03-02 07:41:50.806 | Snyk Open Source |
| High | 696 | Prototype Pollution | [] | ["CWE-1321"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 696 | Regular Expression Denial of Service (ReDoS) | | ["CWE-185","CWE-203"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 696 | Regular Expression Denial of Service (ReDoS) | ["CVE-2021-3807"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Not Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 696 | Prototype Pollution | ["CVE-2020-7699"] | ["CWE-1321"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 696 | Prototype Poisoning | ["CVE-2022-24999"] | ["CWE-1321"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 686 | Prototype Pollution | ["CVE-2019-10744"] | ["CWE-1321"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 686 | Information Exposure | ["CVE-2018-5407"] | ["CWE-203","CWE-204"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | Mature | Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 686 | Improper Input Validation | ["CVE-2018-0494"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | Mature | Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 686 | Prototype Pollution | ["CVE-2020-7788"] | ["CWE-1321"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 686 | Prototype Pollution | ["CVE-2020-35149"] | ["CWE-1321"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 686 | Prototype Pollution | ["CVE-2018-16487"] | ["CWE-1321"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 686 | Prototype Pollution | [] | ["CWE-1321"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 684 | Allocation of Resources Without Limits or Throttling | [] | ["CWE-770"] | e-corp-demo/container-breaking-in-goof(main) | | Not Auto Fixable | 2023-03-02 07:41:52.624 | Snyk Code |
| High | 681 | Command Injection | ["CVE-2021-23337"] | ["CWE-78"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 675 | Deserialization of Untrusted Data | ["CVE-2019-14540"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | Mature | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| Critical | 675 | Remote Code Execution (RCE) | ["CVE-2021-45046"] | ["CWE-94"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Proof of Concept | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Critical | 675 | Remote Code Execution (RCE) | ["CVE-2021-45046"] | ["CWE-94"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-client/pom.xml | Proof of Concept | Auto Fixable | 2023-03-07 21:11:10.235 | Snyk Open Source |
| Critical | 675 | Remote Code Execution (RCE) | ["CVE-2021-45046"] | ["CWE-94"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/pom.xml | Proof of Concept | Auto Fixable | 2023-03-07 21:11:12.255 | Snyk Open Source |
| High | 671 | Prototype Pollution | ["CVE-2022-2564","CVE-2022-24304"] | ["CWE-1321"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 670 | Allocation of Resources Without Limits or Throttling | [] | ["CWE-770"] | e-corp-demo/goof-kubernetes(master) | | Not Auto Fixable | 2023-03-07 23:04:24.374 | Snyk Code |
| Medium | 670 | Allocation of Resources Without Limits or Throttling | [] | ["CWE-770"] | e-corp-demo/goof-kubernetes(master) | | Not Auto Fixable | 2023-03-07 23:04:24.374 | Snyk Code |
| Medium | 670 | Allocation of Resources Without Limits or Throttling | [] | ["CWE-770"] | e-corp-demo/goof-kubernetes(master) | | Not Auto Fixable | 2023-03-07 23:04:24.374 | Snyk Code |
| Medium | 655 | Deserialization of Untrusted Data | ["CVE-2015-6420"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | Proof of Concept | Not Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|-----------------------------------|---|--------------|---|------------------|------------------|----------------------------|------------------|
| Medium | 655 | Deserialization of Untrusted Data | ["CVE-2015-6420"] | ["CWE-502"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/pom.xml | Proof of Concept | Auto Fixable | 2023-03-07 21:11:12.255 | Snyk Open Source |
| High | 654 | Cross-site Scripting (XSS) | ["CVE-2016-10531"] | ["CWE-79"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 644 | Open Redirect | ["CVE-2017-16224"] | ["CWE-601"] | e-corp-demo/goof-kubernetes(master):package.json | Mature | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 644 | Code Injection | [] | ["CWE-95"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 641 | Remote Memory Exposure | [] | ["CWE-201"] | e-corp-demo/goof-kubernetes(master):package.json | Mature | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Critical | 640 | Arbitrary Code Execution | ["CVE-2016-3082"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Critical | 640 | Directory Traversal | ["CVE-2016-6795"] | ["CWE-94"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Critical | 640 | Remote Code Execution | ["CVE-2022-22965"] | ["CWE-94"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | Mature | Not Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| Critical | 640 | Deserialization of Untrusted Data | ["CVE-2015-7501","CVE-2015-4852"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Mature | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Critical | 640 | Arbitrary Code Execution | ["CVE-2016-1000031"] | ["CWE-284"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Critical | 640 | Improper Action Name Cleanup | ["CVE-2016-4436"] | ["CWE-459"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Critical | 640 | User Impersonation | ["CVE-2018-1000134"] | ["CWE-284"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.255 | Snyk Open Source |
| Medium | 636 | Prototype Pollution | ["CVE-2018-3721"] | ["CWE-1321"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 636 | Prototype Pollution | ["CVE-2018-3728"] | ["CWE-1321"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 630 | Deserialization of Untrusted Data | ["CVE-2017-7525"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | Proof of Concept | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 630 | Deserialization of Untrusted Data | ["CVE-2020-36188"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | Proof of Concept | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 630 | Deserialization of Untrusted Data | ["CVE-2017-17485"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | Proof of Concept | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 630 | Deserialization of Untrusted Data | ["CVE-2020-36181"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | Proof of Concept | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 630 | Deserialization of Untrusted Data | ["CVE-2019-12814"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | Proof of Concept | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 630 | Deserialization of Untrusted Data | ["CVE-2020-36179"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | Proof of Concept | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 630 | Deserialization of Untrusted Data | ["CVE-2020-9546","CVE-2020-9547","CVE-2020-9548"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | Proof of Concept | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 630 | Deserialization of Untrusted Data | ["CVE-2020-10673"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | Proof of Concept | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 630 | Deserialization of Untrusted Data | ["CVE-2020-36180"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | Proof of Concept | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 630 | Deserialization of Untrusted Data | ["CVE-2019-14892","CVE-2019-14893"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | Proof of Concept | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 630 | Deserialization of Untrusted Data | ["CVE-2020-36184"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | Proof of Concept | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 630 | Deserialization of Untrusted Data | ["CVE-2019-12086"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | Proof of Concept | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 630 | Deserialization of Untrusted Data | ["CVE-2020-35728"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | Proof of Concept | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|----------------------|-----------------------------------|---|------------------|------------------|----------------------------|------------------|
| High | 630 | Deserialization of Untrusted Data | ["CVE-2020-8840"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | Proof of Concept | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 630 | Deserialization of Untrusted Data | ["CVE-2020-24616"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | Proof of Concept | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 630 | Deserialization of Untrusted Data | ["CVE-2020-36182"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | Proof of Concept | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 630 | Remote Code Execution (RCE) | ["CVE-2021-31805"] | ["CWE-94"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Proof of Concept | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 630 | Deserialization of Untrusted Data | ["CVE-2020-11113"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | Proof of Concept | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 625 | GPL-2.0 license | [] | [] | e-corp-demo/goof-kubernetes(master):package.json | No Data | Not Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 619 | Arbitrary Code Execution | [] | ["CWE-94"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 619 | Arbitrary Code Execution | ["CVE-2017-1000228"] | ["CWE-94"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 614 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2022-0778"] | ["CWE-835"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 614 | Integer Overflow or Wraparound | ["CVE-2021-23840"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 614 | Use After Free | ["CVE-2020-35512"] | ["CWE-416"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 614 | Out-of-bounds Write | ["CVE-2019-13307"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| High | 614 | Out-of-bounds Read | ["CVE-2019-13391"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| High | 614 | NULL Pointer Dereference | ["CVE-2020-17525"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 614 | NULL Pointer Dereference | ["CVE-2018-1000121"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 614 | Out-of-bounds Write | ["CVE-2021-3517"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 614 | Use After Free | ["CVE-2017-15412"] | ["CWE-416"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| High | 614 | Out-of-bounds Write | ["CVE-2019-5436"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| High | 614 | Memory Leak | ["CVE-2019-20388"] | ["CWE-401"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 614 | Improper Initialization | ["CVE-2019-12979"] | ["CWE-665"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| High | 614 | Use After Free | ["CVE-2022-23308"] | ["CWE-416"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 614 | Out-of-bounds Read | ["CVE-2018-8960"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| High | 614 | NULL Pointer Dereference | ["CVE-2017-15015"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| High | 614 | Out-of-bounds Write | ["CVE-2020-8285"] | ["CWE-787", "CWE-327", "CWE-369"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 614 | Use of a Broken or Risky Cryptographic Algorithm | ["CVE-2019-1543"] | ["CWE-327", "CWE-369"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 614 | Divide By Zero | ["CVE-2021-20309"] | ["CWE-369"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| High | 614 | Allocation of Resources Without Limits or Throttling | ["CVE-2017-12429"] | ["CWE-770"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| High | 614 | Memory Leak | ["CVE-2019-20388"] | ["CWE-401"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|---|--------------------|-----------------------|--|------------------|--------------|-------------------------|----------------|
| High | 614 | Out-of-Bounds | ["CVE-2017-15281"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| High | 614 | Out-of-bounds Read | ["CVE-2018-16890"] | ["CWE-125","CWE-74"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 614 | Arbitrary Code Injection | ["CVE-2017-17512"] | ["CWE-74"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 614 | CVE-2018-7738 | ["CVE-2018-7738"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 614 | NULL Pointer Dereference | ["CVE-2017-10790"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| High | 614 | Out-of-bounds Read | ["CVE-2019-11598"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| High | 614 | Resource Exhaustion | ["CVE-2017-12805"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| High | 614 | XML Injection | ["CVE-2020-29599"] | ["CWE-91"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| High | 614 | Improper Certificate Validation | ["CVE-2020-8286"] | ["CWE-295"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| High | 614 | Improper Certificate Validation | ["CVE-2020-8286"] | ["CWE-295"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 614 | Improper Input Validation | ["CVE-2018-13348"] | ["CWE-20"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 614 | Out-of-bounds Write | ["CVE-2020-19667"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| High | 614 | Allocation of Resources Without Limits or Throttling | ["CVE-2017-12435"] | ["CWE-770"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| High | 614 | Out-of-bounds Write | ["CVE-2019-13308"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| High | 614 | Out-of-bounds Write | ["CVE-2020-10543"] | ["CWE-787","CWE-835"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 614 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2022-27781"] | ["CWE-835"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| High | 614 | Out-of-bounds Write | ["CVE-2019-13305"] | ["CWE-787","CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| High | 614 | Missing Release of Resource after Effective Lifetime | ["CVE-2019-19956"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 614 | Missing Release of Resource after Effective Lifetime | ["CVE-2019-19956"] | ["CWE-772"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| High | 614 | Integer Overflow or Wraparound | ["CVE-2020-10878"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 614 | Integer Overflow or Wraparound | ["CVE-2020-27766"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| High | 614 | Improper Encoding or Escaping of Output | ["CVE-2020-26116"] | ["CWE-116"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 614 | Improper Input Validation | ["CVE-2019-20907"] | ["CWE-20"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 614 | Buffer Overflow | ["CVE-2020-12723"] | ["CWE-120"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 614 | Out-of-bounds Write | ["CVE-2019-13306"] | ["CWE-787","CWE-415"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| High | 614 | Double Free | ["CVE-2022-4450"] | ["CWE-415"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| High | 614 | Access of Resource Using Incompatible Type ('Type Confusion') | ["CVE-2023-0286"] | ["CWE-843"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| High | 614 | Use After Free | ["CVE-2022-23308"] | ["CWE-416"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|----------------------|-----------------------|--|------------------|--------------|-------------------------|----------------|
| High | 614 | NULL Pointer Dereference | ["CVE-2017-15017"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| High | 614 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2022-0778"] | ["CWE-835"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 614 | Integer Overflow or Wraparound | ["CVE-2018-20406"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 614 | Use of Uninitialized Resource | ["CVE-2019-13135"] | ["CWE-908"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| High | 614 | Insufficiently Protected Credentials | ["CVE-2020-11008"] | ["CWE-522"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| High | 614 | Out-of-bounds Write | ["CVE-2018-1000035"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 614 | Out-of-bounds Write | ["CVE-2019-13300"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| High | 614 | CVE-2022-27775 | ["CVE-2022-27775"] | [] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| High | 614 | Out-of-Bounds | ["CVE-2019-10131"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| High | 614 | Cleartext Transmission of Sensitive Information | ["CVE-2021-22946"] | ["CWE-319"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| High | 614 | Out-of-bounds Write | ["CVE-2019-13304"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| High | 614 | Improper Ownership Management | ["CVE-2022-29187"] | ["CWE-282","CWE-190"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| High | 614 | Integer Overflow or Wraparound | ["CVE-2021-23840"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 614 | Resource Exhaustion | ["CVE-2021-3737"] | ["CWE-400","CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 614 | Cleartext Transmission of Sensitive Information | ["CVE-2021-22946"] | ["CWE-319"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 614 | Out-of-bounds Read | ["CVE-2019-13295"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| High | 614 | NULL Pointer Dereference | ["CVE-2017-14739"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| High | 614 | CVE-2019-3462 | ["CVE-2019-3462"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 614 | Use After Free | ["CVE-2020-8231"] | ["CWE-416"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 614 | Use After Free | ["CVE-2020-8231"] | ["CWE-416"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| High | 614 | Out-of-bounds Write | ["CVE-2019-5436"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 614 | NULL Pointer Dereference | ["CVE-2019-5010"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 614 | Out-of-Bounds | ["CVE-2017-13090"] | ["CWE-119","CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 614 | Information Exposure | ["CVE-2021-20313"] | ["CWE-200"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| High | 614 | Double Free | ["CVE-2018-8804"] | ["CWE-415"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| High | 614 | Improper Input Validation | ["CVE-2018-13346"] | ["CWE-20"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 614 | Resource Exhaustion | ["CVE-2017-12806"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| High | 614 | Out-of-bounds Read | ["CVE-2019-3823"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|----------------------|------------------|--|------------------|--------------|-------------------------|----------------|
| High | 614 | CVE-2019-16056 | ["CVE-2019-16056"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 614 | Uncontrolled Search Path Element | ["CVE-2022-24765"] | ["CWE-427"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| High | 614 | Out-of-bounds Read | ["CVE-2019-13297"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| High | 614 | Out-of-bounds Write | ["CVE-2017-5130"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| High | 614 | Link Following | ["CVE-2019-12749"] | ["CWE-59"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 614 | Uncontrolled Recursion | ["CVE-2018-6003"] | ["CWE-674"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| High | 614 | Out-of-bounds Write | ["CVE-2017-5130"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 614 | Heap-based Buffer Overflow | ["CVE-2022-39260"] | ["CWE-122","CWE- | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| High | 614 | Improper Certificate Validation | ["CVE-2022-27782"] | ["CWE-295"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| High | 614 | Out-of-Bounds | ["CVE-2017-13089"] | ["CWE-119","CWE- | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 614 | Out-of-bounds Write | ["CVE-2020-8285"] | ["CWE-787","CWE- | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| High | 614 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2017-16932"] | ["CWE-835"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| High | 614 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2017-16932"] | ["CWE-835"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 614 | Out-of-bounds Read | ["CVE-2021-3712"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 614 | Insufficiently Protected Credentials | ["CVE-2020-5260"] | ["CWE-522"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| High | 614 | CVE-2019-16056 | ["CVE-2019-16056"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 614 | Buffer Overflow | ["CVE-2022-28463"] | ["CWE-120"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| High | 614 | Use After Free | ["CVE-2023-0215"] | ["CWE-416"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| High | 614 | Key Management Errors | ["CVE-2018-0732"] | ["CWE-320"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 614 | Out-of-bounds Read | ["CVE-2021-3712"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 614 | Out-of-Bounds | ["CVE-2017-1000254"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 614 | NULL Pointer Dereference | ["CVE-2018-14404"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 614 | NULL Pointer Dereference | ["CVE-2018-14404"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| High | 614 | Use After Free | ["CVE-2021-3516"] | ["CWE-416"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 614 | Use After Free | ["CVE-2021-3516"] | ["CWE-416"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| High | 614 | Integer Overflow or Wraparound | ["CVE-2021-20312"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| High | 614 | Arbitrary Code Injection | ["CVE-2020-8177"] | ["CWE-74"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 614 | Use After Free | ["CVE-2021-3518"] | ["CWE-416"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|------------------------------------|--------------|--|------------------|--------------|-------------------------|------------------|
| High | 614 | Use After Free | ["CVE-2021-3518"] | ["CWE-416"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 614 | Improper Initialization | ["CVE-2019-12977"] | ["CWE-665"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| High | 614 | Cleartext Transmission of Sensitive Information | ["CVE-2021-22946"] | ["CWE-319"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| High | 614 | Use of Incorrectly-Resolved Name or Reference | ["CVE-2018-12020"] | ["CWE-706"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| High | 614 | Arbitrary Code Injection | ["CVE-2020-8177"] | ["CWE-74"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| High | 614 | Allocation of Resources Without Limits or Throttling | ["CVE-2017-12430"] | ["CWE-770"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| High | 614 | Directory Traversal | ["CVE-2023-23946"] | ["CWE-22"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| High | 614 | NULL Pointer Dereference | ["CVE-2017-18209"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| High | 614 | NULL Pointer Dereference | ["CVE-2019-5010"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 614 | Improper Initialization | ["CVE-2019-12978"] | ["CWE-665"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| High | 614 | Out-of-bounds Write | ["CVE-2021-3517"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| High | 614 | Out-of-bounds Read | ["CVE-2019-11597"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| High | 614 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2020-7595"] | ["CWE-835"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| High | 614 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2020-7595"] | ["CWE-835"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 614 | Use After Free | ["CVE-2019-15140"] | ["CWE-416"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| High | 614 | Improper Authentication | ["CVE-2022-22576"] | ["CWE-287"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Medium | 601 | Prototype Pollution | ["CVE-2020-7598"] | ["CWE-1321"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 601 | Prototype Pollution | [] | ["CWE-1321"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 601 | Prototype Pollution | ["CVE-2020-7608"] | ["CWE-1321"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 601 | Prototype Pollution | ["CVE-2019-5428","CVE-2019-11358"] | ["CWE-1321"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 601 | Prototype Pollution | ["CVE-2021-23438"] | ["CWE-1321"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 600 | Denial of Service (DoS) | ["CVE-2021-45105"] | ["CWE-400"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/pom.xml | Proof of Concept | Auto Fixable | 2023-03-07 21:11:12.255 | Snyk Open Source |
| High | 600 | Server-side Template Injection (SSTI) | [] | ["CWE-94"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Proof of Concept | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 600 | Denial of Service (DoS) | ["CVE-2021-45105"] | ["CWE-400"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-client/pom.xml | Proof of Concept | Auto Fixable | 2023-03-07 21:11:10.235 | Snyk Open Source |
| High | 600 | Denial of Service (DoS) | ["CVE-2021-45105"] | ["CWE-400"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Proof of Concept | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 600 | Denial of Service (DoS) | ["CVE-2019-0233"] | ["CWE-400"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Proof of Concept | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Critical | 597 | Prototype Pollution | [] | ["CWE-1321"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 596 | Arbitrary Code Injection | ["CVE-2021-23358"] | ["CWE-94"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|---|----------------------|--------------|---|------------------|------------------|-------------------------|------------------|
| High | 590 | Arbitrary Code Execution | ["CVE-2016-4461"] | ["CWE-264"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 590 | Improper Input Validation | ["CVE-2016-0785"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 590 | Cross-site Request Forgery (CSRF) | ["CVE-2016-4430"] | ["CWE-352"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 590 | Unrestricted Upload of File with Dangerous Type | ["CVE-2012-1592"] | ["CWE-434"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 590 | XML External Entity (XXE) Injection | ["CVE-2014-0225"] | ["CWE-611"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 589 | Regular Expression Denial of Service (ReDoS) | ["CVE-2017-16114"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 589 | Cross-site Scripting (XSS) | [] | ["CWE-79"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 589 | Regular Expression Denial of Service (ReDoS) | ["CVE-2017-16119"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 589 | Regular Expression Denial of Service (ReDoS) | ["CVE-2017-16119"] | ["CWE-400"] | e-corp-demo/container-breaking-in-goof(main):package.json | No Known Exploit | Auto Fixable | 2023-03-02 07:41:50.806 | Snyk Open Source |
| High | 589 | Denial of Service (DoS) | [] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 589 | Regular Expression Denial of Service (ReDoS) | [] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 589 | Denial of Service (DoS) | [] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 589 | Regular Expression Denial of Service (ReDoS) | ["CVE-2016-10540"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 589 | Directory Traversal | ["CVE-2022-24785"] | ["CWE-22"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 589 | Prototype Override Protection Bypass | ["CVE-2017-1000048"] | ["CWE-20"] | e-corp-demo/container-breaking-in-goof(main):package.json | No Known Exploit | Auto Fixable | 2023-03-02 07:41:50.806 | Snyk Open Source |
| High | 589 | Regular Expression Denial of Service (ReDoS) | ["CVE-2016-10539"] | ["CWE-400"] | e-corp-demo/container-breaking-in-goof(main):package.json | No Known Exploit | Auto Fixable | 2023-03-02 07:41:50.806 | Snyk Open Source |
| High | 589 | Regular Expression Denial of Service (ReDoS) | ["CVE-2016-10539"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 589 | Prototype Override Protection Bypass | ["CVE-2017-1000048"] | ["CWE-20"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 589 | Cross-site Scripting (XSS) | ["CVE-2017-1000427"] | ["CWE-79"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 586 | Directory Traversal | ["CVE-2014-3744"] | ["CWE-22"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 586 | Regular Expression Denial of Service (ReDoS) | ["CVE-2022-21680"] | ["CWE-1333"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 586 | Regular Expression Denial of Service (ReDoS) | ["CVE-2020-28500"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 586 | Regular Expression Denial of Service (ReDoS) | ["CVE-2022-21681"] | ["CWE-1333"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 584 | Directory Traversal | [] | ["CWE-22"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 584 | Cross-Site Request Forgery (CSRF) | [] | ["CWE-352"] | e-corp-demo/container-breaking-in-goof(main) | | Not Auto Fixable | 2023-03-02 07:41:52.624 | Snyk Code |
| Medium | 584 | Information Exposure | [] | ["CWE-200"] | e-corp-demo/container-breaking-in-goof(main) | | Not Auto Fixable | 2023-03-02 07:41:52.624 | Snyk Code |
| High | 584 | Regular Expression Denial of Service (ReDoS) | ["CVE-2022-29167"] | ["CWE-1333"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 580 | Reflected File Download | ["CVE-2015-5211"] | ["CWE-494"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|-----------------------------------|----------------------|-------------|---|------------------|------------------|-------------------------|------------------|
| High | 580 | Improper Input Validation | ["CVE-2020-5421"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Medium | 576 | Uninitialized Memory Exposure | [] | ["CWE-201"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 571 | Out-of-Bounds | ["CVE-2017-1000409"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | Mature | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| High | 571 | OS Command Injection | ["CVE-2021-27928"] | ["CWE-78"] | e-corp-demo/goof-kubernetes(master):Dockerfile | Mature | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 568 | SQL Injection | ["CVE-2020-25638"] | ["CWE-89"] | e-corp-demo/java-goof(main):todolist-goof/todolist-core/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:13.069 | Snyk Open Source |
| High | 563 | Deserialization of Untrusted Data | ["CVE-2020-10969"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 563 | Deserialization of Untrusted Data | ["CVE-2020-11111"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 563 | Deserialization of Untrusted Data | ["CVE-2020-10968"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 563 | Deserialization of Untrusted Data | ["CVE-2020-36189"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 563 | Deserialization of Untrusted Data | ["CVE-2020-14060"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 563 | Deserialization of Untrusted Data | ["CVE-2020-14061"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 563 | Deserialization of Untrusted Data | ["CVE-2020-11620"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 563 | Deserialization of Untrusted Data | ["CVE-2020-24750"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 563 | Deserialization of Untrusted Data | ["CVE-2018-14719"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 563 | Deserialization of Untrusted Data | ["CVE-2020-36187"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 563 | Deserialization of Untrusted Data | ["CVE-2018-14720"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 563 | Deserialization of Untrusted Data | ["CVE-2020-14062"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 563 | Deserialization of Untrusted Data | ["CVE-2018-12023"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 563 | Deserialization of Untrusted Data | ["CVE-2020-11112"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 563 | Deserialization of Untrusted Data | ["CVE-2018-19361"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 563 | Deserialization of Untrusted Data | ["CVE-2020-11619"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 563 | Deserialization of Untrusted Data | ["CVE-2020-10650"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 563 | Deserialization of Untrusted Data | ["CVE-2018-19360"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 563 | Deserialization of Untrusted Data | ["CVE-2020-14195"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 563 | Deserialization of Untrusted Data | ["CVE-2018-12022"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 563 | Deserialization of Untrusted Data | ["CVE-2020-36185"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 563 | Deserialization of Untrusted Data | ["CVE-2018-14718"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 563 | Deserialization of Untrusted Data | ["CVE-2018-19362"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|---|-------------------------------------|-----------------------|---|------------------|------------------|-------------------------|------------------|
| High | 563 | Deserialization of Untrusted Data | ["CVE-2020-36183"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 563 | Deserialization of Untrusted Data | ["CVE-2018-11307"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 563 | Deserialization of Untrusted Data | ["CVE-2018-14721"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 563 | Deserialization of Untrusted Data | ["CVE-2020-36186"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 563 | Deserialization of Untrusted Data | [] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 563 | Deserialization of Untrusted Data | ["CVE-2020-10672"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 560 | XML External Entity (XXE) Injection | ["CVE-2020-25649"] | ["CWE-611"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| Medium | 557 | Information Exposure | [] | ["CWE-200"] | e-corp-demo/goof-kubernetes(master) | | Not Auto Fixable | 2023-03-07 23:04:24.374 | Snyk Code |
| Medium | 557 | Cleartext Transmission of Sensitive Information | [] | ["CWE-319"] | e-corp-demo/goof-kubernetes(master) | | Not Auto Fixable | 2023-03-07 23:04:24.374 | Snyk Code |
| Medium | 557 | Cross-Site Request Forgery (CSRF) | [] | ["CWE-352"] | e-corp-demo/goof-kubernetes(master) | | Not Auto Fixable | 2023-03-07 23:04:24.374 | Snyk Code |
| High | 555 | Deserialization of Untrusted Data | ["CVE-2019-12384"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Mature | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 555 | Deserialization of Untrusted Data | ["CVE-2019-16335"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 555 | SQL Injection | ["CVE-2019-14900"] | ["CWE-89"] | e-corp-demo/java-goof(main):todolist-goof/todolist-core/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:13.069 | Snyk Open Source |
| High | 555 | Deserialization of Untrusted Data | ["CVE-2018-7489"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 555 | Deserialization of Untrusted Data | ["CVE-2019-17267"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 555 | Deserialization of Untrusted Data | ["CVE-2019-16943"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 555 | Deserialization of Untrusted Data | ["CVE-2017-15095"] | ["CWE-184"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 555 | Deserialization of Untrusted Data | ["CVE-2021-20190"] | ["CWE-502","CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 555 | Deserialization of Untrusted Data | ["CVE-2020-35490"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 555 | Deserialization of Untrusted Data | ["CVE-2019-17531"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| Medium | 555 | Arbitrary Code Execution | ["CVE-2021-44832"] | ["CWE-94"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Proof of Concept | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Medium | 555 | Arbitrary Code Execution | ["CVE-2021-44832"] | ["CWE-94"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/pom.xml | Proof of Concept | Auto Fixable | 2023-03-07 21:11:12.255 | Snyk Open Source |
| Medium | 555 | Arbitrary Code Execution | ["CVE-2021-44832"] | ["CWE-94"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-client/pom.xml | Proof of Concept | Auto Fixable | 2023-03-07 21:11:10.235 | Snyk Open Source |
| High | 555 | Deserialization of Untrusted Data | ["CVE-2019-20330"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 555 | Deserialization of Untrusted Data | ["CVE-2019-14379","CVE-2019-14439"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 555 | Deserialization of Untrusted Data | ["CVE-2019-16942"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 555 | Deserialization of Untrusted Data | ["CVE-2020-35491"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 555 | Deserialization of Untrusted Data | ["CVE-2018-5968"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|----------------------|----------------------|---|------------------|------------------|-------------------------|------------------|
| High | 550 | Remote Code Execution (RCE) | ["CVE-2022-41853"] | ["CWE-94"] | e-corp-demo/java-goof(main):todolist-goof/todolist-core/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:13.069 | Snyk Open Source |
| High | 546 | Denial of Service (DoS) | ["CVE-2022-24434"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):package.json | Mature | Not Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 546 | Denial of Service (DoS) | ["CVE-2022-24434"] | ["CWE-400"] | e-corp-demo/container-breaking-in-goof(main):package.json | Mature | Not Auto Fixable | 2023-03-02 07:41:50.806 | Snyk Open Source |
| Medium | 541 | Regular Expression Denial of Service (ReDoS) | ["CVE-2019-1010266"] | ["CWE-185"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 539 | Timing Attack | [] | ["CWE-310"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 535 | Directory Traversal | ["CVE-2021-29425"] | ["CWE-22", "CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Mature | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Medium | 526 | Arbitrary Code Injection | [] | ["CWE-94"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 525 | Denial of Service (DoS) | ["CVE-2017-9787"] | ["CWE-400"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 525 | Denial of Service (DoS) | ["CVE-2017-9793"] | ["CWE-400"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 525 | Access Restriction Bypass | ["CVE-2016-4433"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 525 | Denial of Service (DoS) | ["CVE-2021-3859"] | ["CWE-400"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.255 | Snyk Open Source |
| High | 525 | Denial of Service (DoS) | ["CVE-2016-3092"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Medium | 525 | Allocation of Resources Without Limits or Throttling | ["CVE-2023-20863"] | ["CWE-770"] | e-corp-demo/java-goof(main):todolist-goof/todolist-core/pom.xml | No Known Exploit | Auto Fixable | 2023-04-14 20:31:47.627 | Snyk Open Source |
| High | 525 | Improper Certificate Validation | ["CVE-2022-4492"] | ["CWE-295"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.255 | Snyk Open Source |
| High | 525 | Deserialization of Untrusted Data | ["CVE-2019-14540"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Mature | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Medium | 525 | Allocation of Resources Without Limits or Throttling | ["CVE-2023-20863"] | ["CWE-770"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Auto Fixable | 2023-04-15 00:19:59.806 | Snyk Open Source |
| High | 525 | Denial of Service (DoS) | ["CVE-2017-9804"] | ["CWE-400"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 525 | Manipulation of Struts' internals | ["CVE-2015-5209"] | ["CWE-284"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 525 | Access Restriction Bypass | ["CVE-2016-4431"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 525 | Denial of Service (DoS) | ["CVE-2020-36518"] | ["CWE-400"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 525 | Access Restriction Bypass | ["CVE-2016-4433"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 525 | Denial of Service (DoS) | ["CVE-2022-1319"] | ["CWE-400"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.255 | Snyk Open Source |
| High | 525 | Parameter Alteration | ["CVE-2015-5209"] | ["CWE-235"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Medium | 520 | Denial of Service (DoS) | ["CVE-2022-42003"] | ["CWE-400"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | Proof of Concept | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| Medium | 520 | Regular Expression Denial of Service (ReDoS) | [] | ["CWE-1333"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 520 | Denial of Service (DoS) | ["CVE-2022-42004"] | ["CWE-400"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | Proof of Concept | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 515 | Insecure Defaults | ["CVE-2015-1831"] | ["CWE-453"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Medium | 514 | Allocation of Resources Without Limits or Throttling | ["CVE-2017-18258"] | ["CWE-770"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|----------------------|-----------------------|--|------------------|--------------|-------------------------|----------------|
| Medium | 514 | Reachable Assertion | ["CVE-2017-18252"] | ["CWE-617"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Inadequate Encryption Strength | ["CVE-2022-2097"] | ["CWE-326"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Medium | 514 | Out-of-bounds Read | ["CVE-2020-25674"] | ["CWE-125","CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Integer Overflow or Wraparound | ["CVE-2020-27770"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Out-of-bounds Read | ["CVE-2020-25665"] | ["CWE-125","CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Out-of-Bounds | ["CVE-2017-1000101"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Medium | 514 | CVE-2019-1547 | ["CVE-2019-1547"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 514 | Resource Exhaustion | ["CVE-2017-12140"] | ["CWE-400","CWE-327"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Use of a Broken or Risky Cryptographic Algorithm | ["CVE-2018-0737"] | ["CWE-327"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 514 | Out-of-bounds Write | ["CVE-2022-32208"] | ["CWE-787"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Medium | 514 | NULL Pointer Dereference | ["CVE-2017-14060"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Unchecked Return Value | ["CVE-2018-16643"] | ["CWE-252"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Divide By Zero | ["CVE-2020-27760"] | ["CWE-369"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Cross-site Scripting (XSS) | ["CVE-2019-16935"] | ["CWE-79"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 514 | Resource Exhaustion | ["CVE-2017-17682"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Integer Overflow or Wraparound | ["CVE-2021-23841"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 514 | Insufficient Verification of Data Authenticity | ["CVE-2021-22947"] | ["CWE-345"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Medium | 514 | Insufficient Verification of Data Authenticity | ["CVE-2021-22947"] | ["CWE-345"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Medium | 514 | Improper Input Validation | ["CVE-2020-3810"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Medium | 514 | Improper Input Validation | ["CVE-2020-3810"] | ["CWE-20"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.449 | Snyk Container |
| Medium | 514 | Excessive Iteration | ["CVE-2017-14175"] | ["CWE-834"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Reachable Assertion | ["CVE-2017-13658"] | ["CWE-617"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | HTTP Request Smuggling | ["CVE-2021-23336"] | ["CWE-444"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 514 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2018-18024"] | ["CWE-835"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Link Following | ["CVE-2022-39253"] | ["CWE-59"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Medium | 514 | Improper Resource Shutdown or Release | ["CVE-2020-12049"] | ["CWE-404"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Medium | 514 | CVE-2022-4304 | ["CVE-2022-4304"] | [] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Medium | 514 | NULL Pointer Dereference | ["CVE-2021-3596"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|--------------------|-------------|--|------------------|--------------|-------------------------|----------------|
| Medium | 514 | Divide By Zero | ["CVE-2021-20243"] | ["CWE-369"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Link Following | ["CVE-2023-22490"] | ["CWE-59"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Medium | 514 | Use of a Broken or Risky Cryptographic Algorithm | ["CVE-2018-0734"] | ["CWE-327"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 514 | Information Exposure | ["CVE-2021-22876"] | ["CWE-200"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Medium | 514 | Excessive Iteration | ["CVE-2017-14174"] | ["CWE-834"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Allocation of Resources Without Limits or Throttling | ["CVE-2017-13133"] | ["CWE-770"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Use of a Broken or Risky Cryptographic Algorithm | ["CVE-2018-0735"] | ["CWE-327"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 514 | NULL Pointer Dereference | ["CVE-2017-5969"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 514 | Insufficiently Protected Credentials | ["CVE-2022-27774"] | ["CWE-522"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Medium | 514 | Allocation of Resources Without Limits or Throttling | ["CVE-2017-12643"] | ["CWE-770"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | NULL Pointer Dereference | ["CVE-2019-12974"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Allocation of Resources Without Limits or Throttling | ["CVE-2023-23916"] | ["CWE-770"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Medium | 514 | Information Exposure | ["CVE-2019-1551"] | ["CWE-200"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 514 | Divide By Zero | ["CVE-2019-13454"] | ["CWE-369"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2018-20467"] | ["CWE-835"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Out-of-bounds Write | ["CVE-2022-0529"] | ["CWE-787"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Medium | 514 | NULL Pointer Dereference | ["CVE-2020-1971"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 514 | NULL Pointer Dereference | ["CVE-2020-1971"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 514 | Information Exposure | ["CVE-2021-22876"] | ["CWE-200"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Medium | 514 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2018-14567"] | ["CWE-835"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 514 | Divide By Zero | ["CVE-2021-20241"] | ["CWE-369"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Cross-site Scripting (XSS) | ["CVE-2019-16935"] | ["CWE-79"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 514 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2018-20482"] | ["CWE-835"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 514 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2018-20482"] | ["CWE-835"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 514 | Resource Exhaustion | ["CVE-2020-14422"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 514 | Allocation of Resources Without Limits or Throttling | ["CVE-2017-12563"] | ["CWE-770"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Information Exposure | ["CVE-2021-3426"] | ["CWE-200"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 514 | Allocation of Resources Without Limits or Throttling | ["CVE-2017-12692"] | ["CWE-770"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|----------------------|-------------|--|------------------|--------------|-------------------------|----------------|
| Medium | 514 | Out-of-Bounds | ["CVE-2017-3735"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 514 | Arbitrary Code Injection | ["CVE-2019-18348"] | ["CWE-74"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 514 | Information Exposure | ["CVE-2017-1000100"] | ["CWE-200"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Medium | 514 | Excessive Iteration | ["CVE-2017-17914"] | ["CWE-834"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | NULL Pointer Dereference | ["CVE-2017-13768"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Resource Exhaustion | ["CVE-2017-1000476"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Allocation of Resources Without Limits or Throttling | ["CVE-2022-32206"] | ["CWE-770"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Medium | 514 | Out-of-bounds Write | ["CVE-2019-5188"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Medium | 514 | NULL Pointer Dereference | ["CVE-2017-14505"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Allocation of Resources Without Limits or Throttling | ["CVE-2017-12875"] | ["CWE-770"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | CRLF Injection | ["CVE-2019-9947"] | ["CWE-93"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 514 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2017-18273"] | ["CWE-835"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion') | ["CVE-2021-3541"] | ["CWE-776"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 514 | Out-of-bounds Write | ["CVE-2019-5094"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Medium | 514 | XML External Entity (XXE) Injection | ["CVE-2016-9318"] | ["CWE-611"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 514 | Excessive Iteration | ["CVE-2018-9133"] | ["CWE-834"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Divide By Zero | ["CVE-2021-20246"] | ["CWE-369"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Integer Overflow or Wraparound | ["CVE-2022-29824"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 514 | Integer Overflow or Wraparound | ["CVE-2022-29824"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 514 | Integer Overflow or Wraparound | ["CVE-2020-25676"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Information Exposure | ["CVE-2018-0495"] | ["CWE-203"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Medium | 514 | Out-of-bounds Read | ["CVE-2020-24977"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 514 | Out-of-bounds Read | ["CVE-2020-24977"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 514 | Divide By Zero | ["CVE-2020-27750"] | ["CWE-369"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Out-of-bounds Write | ["CVE-2019-5188"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Medium | 514 | Divide By Zero | ["CVE-2021-20176"] | ["CWE-369"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Divide By Zero | ["CVE-2017-14249"] | ["CWE-369"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|--------------------|------------------------|--|------------------|--------------|-------------------------|----------------|
| Medium | 514 | Resource Exhaustion | ["CVE-2019-11470"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Integer Overflow or Wraparound | ["CVE-2020-27350"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.449 | Snyk Container |
| Medium | 514 | Integer Overflow or Wraparound | ["CVE-2020-27350"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Medium | 514 | Resource Exhaustion | ["CVE-2020-8492"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 514 | Improper Input Validation | ["CVE-2018-20852"] | ["CWE-20"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 514 | Use of a Broken or Risky Cryptographic Algorithm | ["CVE-2021-40528"] | ["CWE-327"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 514 | Information Exposure | ["CVE-2017-3738"] | ["CWE-200"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 514 | Resource Exhaustion | ["CVE-2021-3733"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 514 | Integer Overflow or Wraparound | ["CVE-2017-14173"] | ["CWE-190", "CWE-369"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Divide By Zero | ["CVE-2021-20244"] | ["CWE-369"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2017-14741"] | ["CWE-835"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2018-14567"] | ["CWE-835"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 514 | CRLF Injection | ["CVE-2019-9740"] | ["CWE-93"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 514 | Divide By Zero | ["CVE-2019-14981"] | ["CWE-369"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | CRLF Injection | ["CVE-2019-9740"] | ["CWE-93"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 514 | CRLF Injection | ["CVE-2019-9947"] | ["CWE-93"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 514 | Improper Input Validation | ["CVE-2018-20852"] | ["CWE-20"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 514 | Improper Input Validation | ["CVE-2017-13061"] | ["CWE-20"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2018-10177"] | ["CWE-835"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Insufficient Verification of Data Authenticity | ["CVE-2021-22947"] | ["CWE-345"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Medium | 514 | Use After Free | ["CVE-2022-43552"] | ["CWE-416"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Medium | 514 | Out-of-bounds Read | ["CVE-2018-18025"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | NULL Pointer Dereference | ["CVE-2017-14400"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Allocation of Resources Without Limits or Throttling | ["CVE-2018-7443"] | ["CWE-770"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Use of a Broken or Risky Cryptographic Algorithm | ["CVE-2021-40528"] | ["CWE-327"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Medium | 514 | CVE-2022-0530 | ["CVE-2022-0530"] | [] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Medium | 514 | Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion') | ["CVE-2021-3541"] | ["CWE-776"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|----------------------|-------------|--|------------------|------------------|-------------------------|----------------|
| Medium | 514 | XML External Entity (XXE) Injection | ["CVE-2016-9318"] | ["CWE-611"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 514 | Excessive Iteration | ["CVE-2017-14172"] | ["CWE-834"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Divide By Zero | ["CVE-2021-20245"] | ["CWE-369"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | HTTP Request Smuggling | ["CVE-2021-23336"] | ["CWE-444"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 514 | Uncontrolled Recursion | ["CVE-2018-0739"] | ["CWE-674"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 514 | Excessive Iteration | ["CVE-2017-12674"] | ["CWE-834"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Allocation of Resources Without Limits or Throttling | ["CVE-2017-12691"] | ["CWE-770"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | NULL Pointer Dereference | ["CVE-2017-1000445"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Out-of-bounds Write | ["CVE-2020-15999"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | Mature | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Medium | 514 | Out-of-bounds Write | ["CVE-2020-15999"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | Mature | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Medium | 514 | Insufficiently Protected Credentials | ["CVE-2022-27776"] | ["CWE-522"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Medium | 514 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2017-17681"] | ["CWE-835"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Unchecked Return Value | ["CVE-2021-4189"] | ["CWE-252"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 514 | NULL Pointer Dereference | ["CVE-2018-16749"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Information Exposure | ["CVE-2017-3736"] | ["CWE-200"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 514 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2017-18271"] | ["CWE-835"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | NULL Pointer Dereference | ["CVE-2021-3537"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 514 | NULL Pointer Dereference | ["CVE-2021-3537"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 514 | Use After Free | ["CVE-2017-14528"] | ["CWE-416"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Out-of-bounds Read | ["CVE-2019-15139"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Allocation of Resources Without Limits or Throttling | ["CVE-2022-32205"] | ["CWE-770"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Medium | 514 | Link Following | ["CVE-2019-3902"] | ["CWE-59"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 514 | Integer Overflow or Wraparound | ["CVE-2021-23841"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 514 | Allocation of Resources Without Limits or Throttling | ["CVE-2017-18258"] | ["CWE-770"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 514 | Allocation of Resources Without Limits or Throttling | ["CVE-2017-12693"] | ["CWE-770"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Integer Overflow or Wraparound | ["CVE-2020-27762"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | CVE-2018-0733 | ["CVE-2018-0733"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 514 | Divide By Zero | ["CVE-2019-11472"] | ["CWE-369"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|----------------------|------------------------|--|------------------|------------------|-------------------------|------------------|
| Medium | 514 | NULL Pointer Dereference | ["CVE-2017-5969"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 514 | Resource Exhaustion | ["CVE-2017-14341"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 514 | Information Exposure | ["CVE-2019-1551"] | ["CWE-200"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 512 | Arbitrary Code Execution | ["CVE-2019-20920"] | ["CWE-94"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 509 | Denial of Service (DoS) | [] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 509 | Information Exposure | ["CVE-2019-17426"] | ["CWE-200"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 509 | Regular Expression Denial of Service (ReDoS) | [] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 509 | Cross-site Scripting (XSS) | ["CVE-2017-1000188"] | ["CWE-79"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 509 | Denial of Service (DoS) | ["CVE-2017-1000189"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 507 | HTTP Request Smuggling | ["CVE-2020-8287"] | ["CWE-444"] | e-corp-demo/goof-kubernetes(master):Dockerfile | Proof of Concept | Not Auto Fixable | 2023-03-07 23:04:19.457 | Snyk Container |
| Medium | 507 | Use of Hardcoded Credentials | [] | ["CWE-798", "CWE-400"] | e-corp-demo/goof-kubernetes(master) | | Not Auto Fixable | 2023-03-07 23:04:24.374 | Snyk Code |
| High | 507 | Privilege Escalation | ["CVE-2021-22921"] | ["CWE-264"] | e-corp-demo/goof-kubernetes(master):Dockerfile | Proof of Concept | Not Auto Fixable | 2023-03-07 23:04:19.457 | Snyk Container |
| Low | 506 | Prototype Pollution | ["CVE-2021-44906"] | ["CWE-1321"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Low | 506 | Regular Expression Denial of Service (ReDoS) | ["CVE-2018-1109"] | ["CWE-185", "CWE-400"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Low | 506 | Regular Expression Denial of Service (ReDoS) | ["CVE-2017-16137"] | ["CWE-400"] | e-corp-demo/container-breaking-in-goof(main):package.json | Proof of Concept | Auto Fixable | 2023-03-02 07:41:50.806 | Snyk Open Source |
| Low | 506 | Regular Expression Denial of Service (ReDoS) | ["CVE-2017-16137"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 505 | Deserialization of Untrusted Data | ["CVE-2015-6420"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Proof of Concept | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Critical | 500 | Buffer Overflow | ["CVE-2020-26154"] | ["CWE-120"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Critical | 500 | Integer Overflow or Wraparound | ["CVE-2022-3515"] | ["CWE-190"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Critical | 500 | Out-of-bounds Read | ["CVE-2020-36331"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Critical | 500 | Out-of-bounds Read | ["CVE-2019-3860"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Critical | 500 | Race Condition | ["CVE-2019-12450"] | ["CWE-362", "CWE-400"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Critical | 500 | Double Free | ["CVE-2018-16402"] | ["CWE-415"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Critical | 500 | NULL Pointer Dereference | ["CVE-2018-16428"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Critical | 500 | Double Free | ["CVE-2018-16402"] | ["CWE-415"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Critical | 500 | Release of Invalid Pointer or Reference | ["CVE-2021-30473"] | ["CWE-763"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Critical | 500 | Out-of-Bounds | ["CVE-2015-9262"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Critical | 500 | Integer Overflow or Wraparound | ["CVE-2022-47629"] | ["CWE-190"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|--------------------|-------------|---|------------------|------------------|-------------------------|----------------|
| Critical | 500 | Out-of-bounds Write | ["CVE-2018-25011"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Critical | 500 | Exposure of Resource to Wrong Sphere | ["CVE-2022-25236"] | ["CWE-668"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Critical | 500 | Out-of-Bounds | ["CVE-2017-12562"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Critical | 500 | Out-of-bounds Read | ["CVE-2019-3861"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Critical | 500 | Insufficient Verification of Data Authenticity | ["CVE-2019-17006"] | ["CWE-345"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Critical | 500 | Use of Externally-Controlled Format String | ["CVE-2017-10685"] | ["CWE-134"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Critical | 500 | Out-of-bounds Read | ["CVE-2018-12910"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Critical | 500 | Integer Overflow or Wraparound | ["CVE-2022-25315"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Critical | 500 | Integer Overflow or Wraparound | ["CVE-2022-25315"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Critical | 500 | Out-of-bounds Read | ["CVE-2019-3859"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Critical | 500 | Out-of-Bounds | ["CVE-2017-18269"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Critical | 500 | Out-of-bounds Read | ["CVE-2019-20367"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Critical | 500 | Out-of-bounds Write | ["CVE-2021-3520"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Critical | 500 | SQL Injection | ["CVE-2022-29155"] | ["CWE-89"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Critical | 500 | Out-of-bounds Read | ["CVE-2017-7544"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Critical | 500 | Cleartext Transmission of Sensitive Information | ["CVE-2023-23914"] | ["CWE-319"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Medium | 500 | Container does not drop all default capabilities | [] | [] | e-corp-demo/goof-kubernetes(master):goof-mongo-deployment.yaml | | Not Auto Fixable | 2023-03-07 23:04:06.675 | Snyk IaC |
| Critical | 500 | Cleartext Transmission of Sensitive Information | ["CVE-2023-23914"] | ["CWE-319"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Critical | 500 | Out-of-bounds Write | ["CVE-2018-18311"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 500 | Container does not drop all default capabilities | [] | [] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/k8s/deploy.yaml | | Not Auto Fixable | 2023-03-07 21:11:03.946 | Snyk IaC |
| Medium | 500 | Container does not drop all default capabilities | [] | [] | e-corp-demo/goof-kubernetes(master):goof-deployment.yaml | | Not Auto Fixable | 2023-03-07 23:04:06.635 | Snyk IaC |
| Critical | 500 | Out-of-bounds Read | ["CVE-2022-1587"] | ["CWE-125"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Critical | 500 | Out-of-bounds Read | ["CVE-2018-25013"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Critical | 500 | Out-of-bounds Write | ["CVE-2018-6913"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Critical | 500 | Improper Encoding or Escaping of Output | ["CVE-2022-25235"] | ["CWE-116"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Critical | 500 | Out-of-bounds Write | ["CVE-2021-3520"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Critical | 500 | Integer Overflow or Wraparound | ["CVE-2020-0452"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Critical | 500 | Exposure of Resource to Wrong Sphere | ["CVE-2022-25236"] | ["CWE-668"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|---|--------------------|-----------------------|--|------------------|------------------|-------------------------|----------------|
| Critical | 500 | Integer Overflow or Wraparound | ["CVE-2022-24963"] | ["CWE-190"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Critical | 500 | CVE-2018-3183 | ["CVE-2018-3183"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Critical | 500 | Out-of-bounds Write | ["CVE-2018-14600"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Critical | 500 | CVE-2017-10285 | ["CVE-2017-10285"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Critical | 500 | Out-of-Bounds | ["CVE-2017-15804"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Critical | 500 | SQL Injection | ["CVE-2022-29155"] | ["CWE-89"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Critical | 500 | Improper Encoding or Escaping of Output | ["CVE-2022-25235"] | ["CWE-116"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Critical | 500 | Out-of-bounds Write | ["CVE-2018-11236"] | ["CWE-787","CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Critical | 500 | Out-of-Bounds | ["CVE-2017-14632"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Critical | 500 | Out-of-bounds Read | ["CVE-2018-25010"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Critical | 500 | Integer Overflow or Wraparound | ["CVE-2022-22822"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Critical | 500 | Integer Overflow or Wraparound | ["CVE-2022-22823"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Critical | 500 | Integer Overflow or Wraparound | ["CVE-2022-22823"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Critical | 500 | Integer Overflow or Wraparound | ["CVE-2022-22822"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Critical | 500 | Out-of-Bounds | ["CVE-2017-15670"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Critical | 500 | Integer Overflow or Wraparound | ["CVE-2022-25147"] | ["CWE-190"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Critical | 500 | Off-by-one Error | ["CVE-2018-14599"] | ["CWE-193"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Critical | 500 | Out-of-bounds Write | ["CVE-2022-37434"] | ["CWE-787"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Critical | 500 | Double Free | ["CVE-2017-14952"] | ["CWE-415"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Critical | 500 | Out-of-bounds Read | ["CVE-2020-13112"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Critical | 500 | Out-of-bounds Write | ["CVE-2020-36328"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Critical | 500 | Buffer Overflow | ["CVE-2020-10188"] | ["CWE-120"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Critical | 500 | OS Command Injection | ["CVE-2022-2068"] | ["CWE-78"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Critical | 500 | Out-of-bounds Read | ["CVE-2019-3862"] | ["CWE-125","CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Critical | 500 | Integer Overflow or Wraparound | ["CVE-2022-22824"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Critical | 500 | Integer Overflow or Wraparound | ["CVE-2022-22824"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Critical | 500 | Out-of-bounds Read | ["CVE-2020-12403"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Critical | 500 | Use of Uninitialized Resource | ["CVE-2018-25014"] | ["CWE-908"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--------------------------------|--------------------|---------------------|--|------------------|------------------|-------------------------|----------------|
| Critical | 500 | Out-of-bounds Read | ["CVE-2022-1586"] | ["CWE-125"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Critical | 500 | Out-of-bounds Write | ["CVE-2022-2274"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Critical | 500 | Out-of-bounds Read | ["CVE-2018-25012"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Critical | 500 | Out-of-Bounds | ["CVE-2017-10684"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Critical | 500 | Out-of-bounds Write | ["CVE-2022-2274"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Critical | 500 | Out-of-bounds Read | ["CVE-2018-18313"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Critical | 500 | Integer Overflow or Wraparound | ["CVE-2017-14062"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Critical | 500 | Integer Overflow or Wraparound | ["CVE-2017-14062"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Critical | 500 | Out-of-bounds Write | ["CVE-2018-6797"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Critical | 500 | Buffer Overflow | ["CVE-2021-30475"] | ["CWE-120"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Critical | 500 | Out-of-bounds Read | ["CVE-2018-25009"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Critical | 500 | Out-of-bounds Read | ["CVE-2019-20367"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Critical | 500 | Out-of-Bounds | ["CVE-2018-18312"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Critical | 500 | Integer Overflow or Wraparound | ["CVE-2022-23852"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Critical | 500 | Integer Overflow or Wraparound | ["CVE-2022-23852"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Critical | 500 | Out-of-bounds Read | ["CVE-2017-10989"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Critical | 500 | Buffer Overflow | ["CVE-2021-31535"] | ["CWE-120"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Critical | 500 | Use After Free | ["CVE-2021-30474"] | ["CWE-416"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Critical | 500 | CVE-2017-10346 | ["CVE-2017-10346"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Critical | 500 | Buffer Overflow | ["CVE-2021-31535"] | ["CWE-120"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Critical | 500 | Out-of-Bounds | ["CVE-2018-18314"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Critical | 500 | Out-of-bounds Write | ["CVE-2021-43527"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Critical | 500 | Out-of-bounds Read | ["CVE-2020-36330"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Critical | 500 | Out-of-Bounds | ["CVE-2017-12424"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Critical | 500 | Out-of-Bounds | ["CVE-2017-12424"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Critical | 500 | Improper Input Validation | ["CVE-2020-15180"] | ["CWE-20","CWE-96"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Critical | 500 | Use After Free | ["CVE-2020-36329"] | ["CWE-416"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Critical | 500 | Out-of-bounds Read | ["CVE-2019-3858"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|---|---|--------------|---|------------------|------------------|-------------------------|------------------|
| Critical | 500 | OS Command Injection | ["CVE-2022-2068"] | ["CWE-78"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 492 | Remote Memory Exposure | ["CVE-2020-8244"] | ["CWE-9"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Not Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Critical | 490 | Prototype Pollution | [] | ["CWE-1321"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Critical | 490 | XML External Entity (XXE) Injection | ["CVE-2018-20433"] | ["CWE-611"] | e-corp-demo/java-goof(main):todolist-goof/todolist-core/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:31.069 | Snyk Open Source |
| Critical | 490 | XML External Entity (XXE) Injection | ["CVE-2018-20433"] | ["CWE-611"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Critical | 490 | XML External Entity (XXE) Injection | ["CVE-2018-20433"] | ["CWE-611"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| Medium | 484 | Cross-site Scripting (XSS) | ["CVE-2015-9251","CVE-2017-16012"] | ["CWE-79"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 483 | Cross-site Scripting (XSS) | ["CVE-2019-10219"] | ["CWE-79"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 482 | Regular Expression Denial of Service [] (ReDoS) | | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 480 | Deserialization of Untrusted Data | ["CVE-2020-36181"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Proof of Concept | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 480 | Deserialization of Untrusted Data | ["CVE-2020-36180"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Proof of Concept | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 480 | Deserialization of Untrusted Data | ["CVE-2020-35728"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Proof of Concept | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 480 | Deserialization of Untrusted Data | ["CVE-2020-10673"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Proof of Concept | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 480 | Deserialization of Untrusted Data | ["CVE-2020-9546","CVE-2020-9547","CVE-2020-9548"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Proof of Concept | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 480 | Deserialization of Untrusted Data | ["CVE-2017-17485"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Proof of Concept | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 480 | Deserialization of Untrusted Data | ["CVE-2020-36184"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Proof of Concept | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 480 | Deserialization of Untrusted Data | ["CVE-2019-12086"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Proof of Concept | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 480 | Deserialization of Untrusted Data | ["CVE-2020-24616"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Proof of Concept | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 480 | Deserialization of Untrusted Data | ["CVE-2020-8840"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Proof of Concept | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 480 | Deserialization of Untrusted Data | ["CVE-2020-36182"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Proof of Concept | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 480 | Deserialization of Untrusted Data | ["CVE-2019-14892","CVE-2019-14893"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Proof of Concept | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 480 | Deserialization of Untrusted Data | ["CVE-2019-12814"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Proof of Concept | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 480 | Deserialization of Untrusted Data | ["CVE-2020-36179"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Proof of Concept | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 480 | Deserialization of Untrusted Data | ["CVE-2020-36188"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Proof of Concept | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 480 | Deserialization of Untrusted Data | ["CVE-2020-11113"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Proof of Concept | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 480 | Deserialization of Untrusted Data | ["CVE-2017-7525"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Proof of Concept | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Medium | 479 | Regular Expression Denial of Service [] (ReDoS) | | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|---|----------------------|-------------------|--|------------------|------------------|-------------------------|------------------|
| Medium | 479 | Regular Expression Denial of Service (ReDoS) | ["CVE-2015-8855"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 479 | Regular Expression Denial of Service [] (ReDoS) | | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 479 | Regular Expression Denial of Service (ReDoS) | ["CVE-2015-8315"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 475 | Denial of Service (DoS) | ["CVE-2023-24998"] | ["CWE-400"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Medium | 475 | Information Exposure | [] | ["CWE-200"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 472 | Prototype Pollution | ["CVE-2020-7774"] | ["CWE-1321"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 472 | Arbitrary Code Execution | [] | ["CWE-94"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 471 | Integer Overflow or Wraparound | ["CVE-2023-2004"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-04-15 19:19:14.674 | Snyk Container |
| Medium | 471 | NULL Pointer Dereference | ["CVE-2017-11333"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | Mature | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| High | 471 | Integer Overflow or Wraparound | ["CVE-2023-2004"] | ["CWE-190"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-04-15 19:53:05.953 | Snyk Container |
| Medium | 471 | Cross-site Scripting (XSS) | ["CVE-2020-11022"] | ["CWE-79"] | e-corp-demo/goof-kubernetes(master):Dockerfile | Mature | Not Auto Fixable | 2023-03-07 23:04:19.455 | Snyk Container |
| High | 471 | Out-of-bounds Write | ["CVE-2023-29491"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-04-13 21:35:31.167 | Snyk Container |
| Medium | 471 | Cross-site Scripting (XSS) | ["CVE-2020-11023"] | ["CWE-79"] | e-corp-demo/goof-kubernetes(master):Dockerfile | Mature | Not Auto Fixable | 2023-03-07 23:04:19.455 | Snyk Container |
| High | 471 | Out-of-bounds Write | ["CVE-2023-29491"] | ["CWE-787"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-04-13 17:29:38.601 | Snyk Container |
| Medium | 471 | Information Exposure | ["CVE-2018-5407"] | ["CWE-203", "CWE- | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | Mature | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 471 | CVE-2017-10355 | ["CVE-2017-10355"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | Mature | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 469 | Remote Memory Exposure | ["CVE-2017-16026"] | ["CWE-201"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 465 | Cross-site Request Forgery (CSRF) | ["CVE-2014-0054"] | ["CWE-352"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 457 | Remote Code Execution (RCE) | ["CVE-2021-23369"] | ["CWE-94"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 455 | Cross-site Scripting (XSS) | ["CVE-2016-2162"] | ["CWE-79"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Medium | 455 | Cross-site Scripting (XSS) | ["CVE-2016-4003"] | ["CWE-79"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Medium | 454 | Cross-site Scripting (XSS) | [] | ["CWE-79"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 450 | XML External Entity (XXE) Injection | ["CVE-2018-1000632"] | ["CWE-611"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Proof of Concept | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 450 | XML External Entity (XXE) Injection | ["CVE-2018-1000632"] | ["CWE-611"] | e-corp-demo/java-goof(main):todolist-goof/todolist-core/pom.xml | Proof of Concept | Not Auto Fixable | 2023-03-07 21:11:13.069 | Snyk Open Source |
| High | 450 | Denial of Service (DoS) | ["CVE-2019-5427"] | ["CWE-776"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | Proof of Concept | Not Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 450 | XML External Entity (XXE) Injection | ["CVE-2018-1000632"] | ["CWE-611"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | Proof of Concept | Not Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 450 | Denial of Service (DoS) | ["CVE-2019-5427"] | ["CWE-776"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Proof of Concept | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 450 | Denial of Service (DoS) | ["CVE-2019-5427"] | ["CWE-776"] | e-corp-demo/java-goof(main):todolist-goof/todolist-core/pom.xml | Proof of Concept | Not Auto Fixable | 2023-03-07 21:11:13.069 | Snyk Open Source |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|----------------------|--------------|--|------------------|------------------|-------------------------|------------------|
| Low | 436 | CVE-2023-28484 | ["CVE-2023-28484"] | [] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Auto Fixable | 2023-04-15 19:19:14.675 | Snyk Container |
| Low | 436 | CVE-2023-29469 | ["CVE-2023-29469"] | [] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Auto Fixable | 2023-04-15 19:19:14.675 | Snyk Container |
| Medium | 432 | Prototype Pollution | [] | ["CWE-1321"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 432 | Server-side Request Forgery (SSRF) | ["CVE-2023-28155"] | ["CWE-918"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Not Auto Fixable | 2023-03-18 07:21:27.337 | Snyk Open Source |
| High | 430 | Prototype Pollution | ["CVE-2021-3918"] | ["CWE-1321"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 425 | Denial of Service (DoS) | ["CVE-2015-3192"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Medium | 425 | Arbitrary File Write via Archive Extraction (Zip Slip) | ["CVE-2018-1002201"] | ["CWE-29"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Medium | 425 | MPL-2.0 license | [] | [] | e-corp-demo/goof-kubernetes(master):package.json | No Data | Not Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 418 | SQL Injection | ["CVE-2020-25638"] | ["CWE-89"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 418 | SQL Injection | ["CVE-2020-25638"] | ["CWE-89"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Medium | 415 | Denial of Service (DoS) | ["CVE-2022-22970"] | ["CWE-400"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Medium | 415 | Directory Traversal | ["CVE-2014-3578"] | ["CWE-22"] | e-corp-demo/java-goof(main):todolist-goof/todolist-core/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:13.069 | Snyk Open Source |
| Medium | 415 | Denial of Service (DoS) | ["CVE-2022-2053"] | ["CWE-400"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.255 | Snyk Open Source |
| Medium | 415 | Improper Input Validation | ["CVE-2020-10693"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| Medium | 415 | Denial of Service (DoS) | ["CVE-2022-22970"] | ["CWE-400"] | e-corp-demo/java-goof(main):todolist-goof/todolist-core/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:13.069 | Snyk Open Source |
| Medium | 415 | Regular Expression Denial of Service (ReDoS) | ["CVE-2016-4465"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Medium | 415 | Directory Traversal | ["CVE-2014-3578"] | ["CWE-22"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Medium | 415 | Denial of Service (DoS) | [] | ["CWE-399"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| Medium | 415 | Allocation of Resources Without Limits or Throttling | ["CVE-2022-0084"] | ["CWE-770"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.255 | Snyk Open Source |
| Medium | 415 | Denial of Service (DoS) | ["CVE-2016-3093"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Medium | 415 | JSM bypass via ReflectionHelper | ["CVE-2014-3558"] | ["CWE-592"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| Medium | 415 | Improper Input Validation | ["CVE-2016-3093"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Medium | 415 | Allocation of Resources Without Limits or Throttling | ["CVE-2023-20861"] | ["CWE-770"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Auto Fixable | 2023-03-24 04:58:04.976 | Snyk Open Source |
| Medium | 415 | Allocation of Resources Without Limits or Throttling | ["CVE-2023-20861"] | ["CWE-770"] | e-corp-demo/java-goof(main):todolist-goof/todolist-core/pom.xml | No Known Exploit | Auto Fixable | 2023-03-23 20:29:37.120 | Snyk Open Source |
| Medium | 415 | Denial of Service (DoS) | [] | ["CWE-399"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| Medium | 415 | Denial of Service (DoS) | ["CVE-2022-22950"] | ["CWE-400"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Medium | 415 | Regular Expression Denial of Service (ReDoS) | ["CVE-2016-4465"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Medium | 415 | Denial of Service (DoS) | ["CVE-2022-22950"] | ["CWE-400"] | e-corp-demo/java-goof(main):todolist-goof/todolist-core/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:13.069 | Snyk Open Source |

Sunday 30 April 2023

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|---------------------------------------|-------------------------------------|-----------------------|---|------------------|------------------|-------------------------|------------------|
| High | 413 | Deserialization of Untrusted Data | ["CVE-2020-36186"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Low | 410 | Improper Handling of Case Sensitivity | ["CVE-2022-22968"] | ["CWE-178"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Proof of Concept | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Low | 410 | Improper Handling of Case Sensitivity | ["CVE-2022-22968"] | ["CWE-178"] | e-corp-demo/java-goof(main):todolist-goof/todolist-core/pom.xml | Proof of Concept | Auto Fixable | 2023-03-07 21:11:13.069 | Snyk Open Source |
| High | 410 | XML External Entity (XXE) Injection | ["CVE-2020-25649"] | ["CWE-611"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 405 | Deserialization of Untrusted Data | ["CVE-2019-16335"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 405 | Deserialization of Untrusted Data | ["CVE-2020-35491"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 405 | Deserialization of Untrusted Data | ["CVE-2018-7489"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 405 | Deserialization of Untrusted Data | ["CVE-2017-15095"] | ["CWE-184"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 405 | Deserialization of Untrusted Data | ["CVE-2019-17267"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 405 | Deserialization of Untrusted Data | ["CVE-2019-20330"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 405 | Deserialization of Untrusted Data | ["CVE-2019-16942"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 405 | SQL Injection | ["CVE-2019-14900"] | ["CWE-89"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 405 | Deserialization of Untrusted Data | ["CVE-2019-16943"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 405 | SQL Injection | ["CVE-2019-14900"] | ["CWE-89"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 405 | Deserialization of Untrusted Data | ["CVE-2020-35490"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 405 | Deserialization of Untrusted Data | ["CVE-2019-14379","CVE-2019-14439"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 405 | Deserialization of Untrusted Data | ["CVE-2019-17531"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 405 | Deserialization of Untrusted Data | ["CVE-2021-20190"] | ["CWE-502","CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 405 | Deserialization of Untrusted Data | ["CVE-2018-5968"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 400 | CVE-2022-27449 | ["CVE-2022-27449"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Out-of-bounds Write | ["CVE-2020-19131"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Out-of-Bounds | ["CVE-2021-32027"] | ["CWE-119","CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Arbitrary Command Injection | ["CVE-2015-20107"] | ["CWE-77"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Integer Overflow or Wraparound | ["CVE-2020-0181"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Out-of-bounds Write | ["CVE-2021-3246"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| High | 400 | Double Free | ["CVE-2020-36225"] | ["CWE-415"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Integer Underflow | ["CVE-2020-36221"] | ["CWE-191"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Buffer Overflow | ["CVE-2020-18032"] | ["CWE-120"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|---|--------------------|----------------------|--|------------------|------------------|-------------------------|------------------|
| High | 400 | Improper Authentication | ["CVE-2022-22576"] | ["CWE-287"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 400 | CVE-2022-27451 | ["CVE-2022-27451"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Incomplete Cleanup | ["CVE-2022-1552"] | ["CWE-459","CWE-89"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Resource Exhaustion | ["CVE-2018-20030"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Out-of-Bounds | ["CVE-2017-14160"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| High | 400 | SQL Injection | ["CVE-2021-23214"] | ["CWE-89"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Out-of-bounds Write | ["CVE-2018-21010"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Out-of-Bounds | ["CVE-2020-35524"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Prototype Pollution | ["CVE-2022-21824"] | ["CWE-1321"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.457 | Snyk Container |
| High | 400 | Remote Code Execution (RCE) | ["CVE-2022-41853"] | ["CWE-94"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 400 | CVE-2018-6553 | ["CVE-2018-6553"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 400 | Out-of-bounds Write | ["CVE-2018-11237"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| High | 400 | Out-of-bounds Write | ["CVE-2018-17795"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Improper Input Validation | ["CVE-2018-14598"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| High | 400 | Out-of-bounds Read | ["CVE-2017-9935"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Integer Overflow or Wraparound | ["CVE-2022-22826"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 400 | Out-of-bounds Read | ["CVE-2020-36223"] | ["CWE-125","CWE- | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Out-of-Bounds | ["CVE-2017-6892"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| High | 400 | Reachable Assertion | ["CVE-2021-27212"] | ["CWE-617"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | CVE-2018-2637 | ["CVE-2018-2637"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| High | 400 | Use After Free | ["CVE-2020-13871"] | ["CWE-416"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Reachable Assertion | ["CVE-2020-36222"] | ["CWE-617"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | CVE-2020-36226 | ["CVE-2020-36226"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Integer Overflow or Wraparound | ["CVE-2022-22825"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 400 | Out-of-bounds Write | ["CVE-2019-11745"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| High | 400 | Out-of-bounds Read | ["CVE-2017-12613"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 400 | Cleartext Transmission of Sensitive Information | ["CVE-2022-42916"] | ["CWE-319"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| High | 400 | Out-of-bounds Read | ["CVE-2019-9936"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|---|--------------------|------------------|--|------------------|------------------|-------------------------|----------------|
| High | 400 | Integer Overflow or Wraparound | ["CVE-2017-16612"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| High | 400 | Out-of-bounds Read | ["CVE-2020-13790"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| High | 400 | Incorrect Conversion between Numeric Types | ["CVE-2021-27219"] | ["CWE-681"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 400 | SQL Injection | ["CVE-2022-27380"] | ["CWE-89"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Information Exposure | ["CVE-2018-12886"] | ["CWE-209"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 400 | CVE-2018-3149 | ["CVE-2018-3149"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| High | 400 | Out-of-bounds Read | ["CVE-2020-36223"] | ["CWE-125","CWE- | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Integer Overflow or Wraparound | ["CVE-2020-35523"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | SQL Injection | ["CVE-2020-25695"] | ["CWE-89"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Use After Free | ["CVE-2020-35512"] | ["CWE-416"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| High | 400 | CVE-2020-14583 | ["CVE-2020-14583"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Use After Free | ["CVE-2022-27376"] | ["CWE-416"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Integer Overflow or Wraparound | ["CVE-2021-43618"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| High | 400 | Incorrect Permission Assignment for Critical Resource | ["CVE-2019-13012"] | ["CWE-732"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 400 | Use After Free | ["CVE-2017-7805"] | ["CWE-416"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| High | 400 | Use of a Broken or Risky Cryptographic Algorithm | ["CVE-2021-20305"] | ["CWE-327"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| High | 400 | Use of a Broken or Risky Cryptographic Algorithm | ["CVE-2021-20305"] | ["CWE-327"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Integer Overflow or Wraparound | ["CVE-2020-35523"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Double Free | ["CVE-2022-2509"] | ["CWE-415"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| High | 400 | Out-of-bounds Write | ["CVE-2018-18557"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Out-of-Bounds | ["CVE-2017-17095"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | NULL Pointer Dereference | ["CVE-2017-11113"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| High | 400 | SQL Injection | ["CVE-2022-27384"] | ["CWE-89"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Reachable Assertion | ["CVE-2020-36222"] | ["CWE-617"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Out-of-bounds Read | ["CVE-2019-15903"] | ["CWE-125","CWE- | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 400 | Reachable Assertion | ["CVE-2020-25710"] | ["CWE-617"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Out-of-bounds Write | ["CVE-2018-8905"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Integer Overflow or Wraparound | ["CVE-2020-29361"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|--------------------|------------------------|--|------------------|------------------|-------------------------|----------------|
| High | 400 | Improper Input Validation | ["CVE-2022-1271"] | ["CWE-20"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| High | 400 | Improper Input Validation | ["CVE-2022-1271"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| High | 400 | CVE-2020-2604 | ["CVE-2020-2604"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Resource Exhaustion | ["CVE-2020-12243"] | ["CWE-400"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Resource Exhaustion | ["CVE-2020-12243"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Untrusted Search Path | ["CVE-2017-16997"] | ["CWE-426"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 400 | Out-of-bounds Write | ["CVE-2019-17546"] | ["CWE-787", "CWE-770"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Allocation of Resources Without Limits or Throttling | ["CVE-2017-12944"] | ["CWE-770"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Integer Overflow or Wraparound | ["CVE-2020-29361"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2020-36227"] | ["CWE-835"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Resource Exhaustion | ["CVE-2019-2602"] | ["CWE-400"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| High | 400 | Reachable Assertion | ["CVE-2020-25709"] | ["CWE-617"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | CVE-2019-2698 | ["CVE-2019-2698"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| High | 400 | SQL Injection | ["CVE-2022-27386"] | ["CWE-89"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Double Free | ["CVE-2020-36225"] | ["CWE-415"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | SQL Injection | ["CVE-2022-24407"] | ["CWE-89"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| High | 400 | Authentication Bypass | ["CVE-2017-18190"] | ["CWE-290"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 400 | Use After Free | ["CVE-2020-1712"] | ["CWE-416"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Use After Free | ["CVE-2020-1712"] | ["CWE-416"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Divide By Zero | ["CVE-2017-11464"] | ["CWE-369"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| High | 400 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2022-0778"] | ["CWE-835"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Out-of-bounds Write | ["CVE-2018-16335"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | CVE-2018-2794 | ["CVE-2018-2794"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | NULL Pointer Dereference | ["CVE-2021-20299"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Out-of-bounds Write | ["CVE-2018-17101"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Improper Input Validation | ["CVE-2021-3580"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| High | 400 | Out-of-bounds Write | ["CVE-2021-3500"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| High | 400 | Improper Authentication | ["CVE-2022-22576"] | ["CWE-287"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|--------------------|------------------|--|------------------|------------------|-------------------------|----------------|
| High | 400 | Divide By Zero | ["CVE-2016-9112"] | ["CWE-369"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2022-0778"] | ["CWE-835"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Divide By Zero | ["CVE-2017-11464"] | ["CWE-369"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Link Following | ["CVE-2018-12015"] | ["CWE-59"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | SQL Injection | ["CVE-2022-27385"] | ["CWE-89"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Deserialization of Untrusted Data | ["CVE-2018-15686"] | ["CWE-502"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Out-of-bounds Write | ["CVE-2018-25032"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.457 | Snyk Container |
| High | 400 | SQL Injection | ["CVE-2022-27378"] | ["CWE-89"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | CVE-2022-27452 | ["CVE-2022-27452"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | CVE-2017-10388 | ["CVE-2017-10388"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Out-of-bounds Write | ["CVE-2019-3863"] | ["CWE-787","CWE- | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| High | 400 | Out-of-bounds Read | ["CVE-2018-6798"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2020-36227"] | ["CWE-835"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Use After Free | ["CVE-2020-13630"] | ["CWE-416"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Use After Free | ["CVE-2020-13630"] | ["CWE-416"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | CVE-2018-4180 | ["CVE-2018-4180"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 400 | Out-of-bounds Read | ["CVE-2019-11719"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| High | 400 | Out-of-Bounds | ["CVE-2018-15688"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Out-of-bounds Read | ["CVE-2017-12613"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.449 | Snyk Container |
| High | 400 | CVE-2022-27444 | ["CVE-2022-27444"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Buffer Overflow | ["CVE-2022-27387"] | ["CWE-120"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Out-of-bounds Write | ["CVE-2019-3855"] | ["CWE-787","CWE- | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| High | 400 | Out-of-bounds Write | ["CVE-2019-2201"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Information Exposure | ["CVE-2018-12886"] | ["CWE-209"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| High | 400 | Out-of-bounds Write | ["CVE-2018-12900"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Out-of-bounds Write | ["CVE-2018-12900"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Link Following | ["CVE-2021-26720"] | ["CWE-59"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.449 | Snyk Container |
| High | 400 | Link Following | ["CVE-2021-26720"] | ["CWE-59"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|----------------------|-----------------------|--|------------------|------------------|-------------------------|----------------|
| High | 400 | Improper Enforcement of Message or Data Structure | ["CVE-2020-11080"] | ["CWE-707"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-1000408"] | ["CWE-772"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| High | 400 | Use After Free | ["CVE-2022-40674"] | ["CWE-416"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| High | 400 | Incorrect Conversion between Numeric Types | ["CVE-2021-27219"] | ["CWE-681"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| High | 400 | Integer Overflow or Wraparound | ["CVE-2018-17100"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Out-of-bounds Write | ["CVE-2020-27823"] | ["CWE-787","CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Out-of-bounds Write | ["CVE-2019-19906"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 400 | Integer Overflow or Wraparound | ["CVE-2018-20346"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Improper Certificate Validation | ["CVE-2021-3450"] | ["CWE-295"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.457 | Snyk Container |
| High | 400 | SQL Injection | ["CVE-2022-27385"] | ["CWE-89"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| High | 400 | Use After Free | ["CVE-2021-22940"] | ["CWE-416"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.457 | Snyk Container |
| High | 400 | Out-of-bounds Read | ["CVE-2019-13115"] | ["CWE-125","CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| High | 400 | Out-of-bounds Read | ["CVE-2019-13115"] | ["CWE-125","CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | NULL Pointer Dereference | ["CVE-2019-18804"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| High | 400 | NULL Pointer Dereference | ["CVE-2020-25692"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Use After Free | ["CVE-2022-27458"] | ["CWE-416"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | CRLF Injection | ["CVE-2017-15400"] | ["CWE-93"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 400 | Out-of-bounds Read | ["CVE-2021-3712"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Resource Exhaustion | ["CVE-2020-14152"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Resource Exhaustion | ["CVE-2020-14152"] | ["CWE-400"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| High | 400 | Out-of-bounds Read | ["CVE-2020-13790"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Out-of-bounds Read | ["CVE-2017-12596"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | CVE-2021-2388 | ["CVE-2021-2388"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| High | 400 | Improper Handling of Exceptional Conditions | ["CVE-2019-20218"] | ["CWE-755"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Integer Overflow or Wraparound | ["CVE-2020-14363"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Out-of-bounds Write | ["CVE-2020-25219"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| High | 400 | Buffer Overflow | ["CVE-2019-8696"] | ["CWE-120"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 400 | Use After Free | ["CVE-2022-27383"] | ["CWE-416"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|----------------------|-----------------------|--|------------------|------------------|-------------------------|----------------|
| High | 400 | CVE-2019-9513 | ["CVE-2019-9513"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| High | 400 | Out-of-Bounds | ["CVE-2020-35524"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Allocation of Resources Without Limits or Throttling | ["CVE-2021-46828"] | ["CWE-770"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| High | 400 | Out-of-bounds Read | ["CVE-2017-14246"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| High | 400 | Out-of-Bounds | ["CVE-2019-11729"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| High | 400 | Integer Underflow | ["CVE-2020-36221"] | ["CWE-191"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Improper Handling of Exceptional Conditions | ["CVE-2019-20218"] | ["CWE-755"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Integer Overflow or Wraparound | ["CVE-2020-14363"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| High | 400 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2017-13728"] | ["CWE-835"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| High | 400 | Improper Input Validation | ["CVE-2018-1000168"] | ["CWE-20","CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Release of Invalid Pointer or Reference | ["CVE-2020-36224"] | ["CWE-763"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Use After Free | ["CVE-2022-27377"] | ["CWE-416"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Out-of-bounds Write | ["CVE-2020-19131"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Integer Underflow | ["CVE-2017-6313"] | ["CWE-191"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 400 | Integer Overflow or Wraparound | ["CVE-2021-46143"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| High | 400 | Integer Overflow or Wraparound | ["CVE-2021-46143"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 400 | Out-of-bounds Write | ["CVE-2019-5827"] | ["CWE-787","CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Out-of-bounds Write | ["CVE-2019-3857"] | ["CWE-787","CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| High | 400 | Out-of-bounds Read | ["CVE-2017-14245"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| High | 400 | Integer Overflow or Wraparound | ["CVE-2022-22827"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| High | 400 | Use After Free | ["CVE-2022-27447"] | ["CWE-416"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | CVE-2020-2805 | ["CVE-2020-2805"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Reachable Assertion | ["CVE-2022-27382"] | ["CWE-617"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Integer Overflow or Wraparound | ["CVE-2020-10878"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Off-by-one Error | ["CVE-2021-3999"] | ["CWE-193"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| High | 400 | Integer Overflow or Wraparound | ["CVE-2021-23840"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Out-of-bounds Write | ["CVE-2019-9278"] | ["CWE-787","CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | SQL Injection | ["CVE-2022-27379"] | ["CWE-89"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|----------------------|-----------------------|--|------------------|------------------|-------------------------|----------------|
| High | 400 | CVE-2018-2633 | ["CVE-2018-2633"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| High | 400 | Out-of-bounds Write | ["CVE-2020-0478"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| High | 400 | Integer Overflow or Wraparound | ["CVE-2018-20506"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Integer Overflow or Wraparound | ["CVE-2018-20506"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Integer Overflow or Wraparound | ["CVE-2021-32491"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| High | 400 | Permissive Whitelist | ["CVE-2020-25696"] | ["CWE-183","CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Out-of-bounds Write | ["CVE-2022-0891"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Out-of-bounds Write | ["CVE-2022-0891"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Allocation of Resources Without Limits or Throttling | ["CVE-2018-16865"] | ["CWE-770"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Resource Exhaustion | ["CVE-2020-13114"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Improper Input Validation | ["CVE-2022-1271"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Improper Input Validation | ["CVE-2022-1271"] | ["CWE-20"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.457 | Snyk Container |
| High | 400 | Out-of-bounds Write | ["CVE-2021-32493"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| High | 400 | Integer Overflow or Wraparound | ["CVE-2017-1000422"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 400 | Double Free | ["CVE-2019-3829"] | ["CWE-415","CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| High | 400 | Cleartext Transmission of Sensitive Information | ["CVE-2022-42916"] | ["CWE-319"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| High | 400 | Reachable Assertion | ["CVE-2020-36230"] | ["CWE-617"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Uncontrolled Recursion | ["CVE-2020-28196"] | ["CWE-674"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.455 | Snyk Container |
| High | 400 | Buffer Overflow | ["CVE-2019-8675"] | ["CWE-120"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 400 | Improper Certificate Validation | ["CVE-2022-27782"] | ["CWE-295"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 400 | Integer Overflow or Wraparound | ["CVE-2022-22825"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| High | 400 | Out-of-bounds Write | ["CVE-2018-5146"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| High | 400 | Use After Free | ["CVE-2022-27456"] | ["CWE-416"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | NULL Pointer Dereference | ["CVE-2019-9937"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | CVE-2022-27445 | ["CVE-2022-27445"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Information Exposure | ["CVE-2023-0361"] | ["CWE-203"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| High | 400 | Integer Overflow or Wraparound | ["CVE-2020-10531"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| High | 400 | Incorrect Calculation | ["CVE-2021-45960"] | ["CWE-682"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|----------------------|-----------------------|---|------------------|------------------|-------------------------|------------------|
| High | 400 | Out-of-bounds Write | ["CVE-2021-32490"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| High | 400 | CVE-2017-9113 | ["CVE-2017-9113"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Out-of-bounds Write | ["CVE-2020-8112"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2017-15908"] | ["CWE-835"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | SQL Injection | ["CVE-2022-24407"] | ["CWE-89"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 400 | Integer Overflow or Wraparound | ["CVE-2019-17498"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Integer Overflow or Wraparound | ["CVE-2019-17498"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| High | 400 | Remote Code Execution (RCE) | ["CVE-2022-41853"] | ["CWE-94"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 400 | Use After Free | ["CVE-2022-27457"] | ["CWE-416"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Integer Overflow or Wraparound | ["CVE-2018-17100"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | NULL Pointer Dereference | ["CVE-2020-25692"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Out-of-bounds Read | ["CVE-2021-22918"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.457 | Snyk Container |
| High | 400 | Integer Underflow | ["CVE-2020-36228"] | ["CWE-191"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Integer Underflow | ["CVE-2020-36228"] | ["CWE-191"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Improper Initialization | ["CVE-2020-11655"] | ["CWE-665"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | CVE-2019-13565 | ["CVE-2019-13565"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Out-of-bounds Write | ["CVE-2018-15209"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Out-of-bounds Read | ["CVE-2021-4156"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| High | 400 | Release of Invalid Pointer or Reference | ["CVE-2020-36224"] | ["CWE-763"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Out-of-bounds Write | ["CVE-2020-6851"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Out-of-bounds Write | ["CVE-2018-18444"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Improper Input Validation | ["CVE-2018-1000168"] | ["CWE-20","CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| High | 400 | Allocation of Resources Without Limits or Throttling | ["CVE-2018-16864"] | ["CWE-770"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Out-of-bounds Read | ["CVE-2021-32492"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| High | 400 | CVE-2022-27446 | ["CVE-2022-27446"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Out-of-bounds Write | ["CVE-2019-5827"] | ["CWE-787","CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Untrusted Search Path | ["CVE-2020-14350"] | ["CWE-426"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Reachable Assertion | ["CVE-2020-25709"] | ["CWE-617"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|---|--------------------|-----------------------|--|------------------|------------------|-------------------------|----------------|
| High | 400 | Reachable Assertion | ["CVE-2020-25710"] | ["CWE-617"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | CVE-2020-14593 | ["CVE-2020-14593"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Allocation of Resources Without Limits or Throttling | ["CVE-2019-9511"] | ["CWE-770"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| High | 400 | Improper Authorization | ["CVE-2019-3842"] | ["CWE-285"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Out-of-bounds Write | ["CVE-2017-16879"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| High | 400 | Integer Overflow or Wraparound | ["CVE-2021-43618"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| High | 400 | Access of Resource Using Incompatible Type ('Type Confusion') | ["CVE-2020-36229"] | ["CWE-843"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Access of Resource Using Incompatible Type ('Type Confusion') | ["CVE-2020-36229"] | ["CWE-843"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Reachable Assertion | ["CVE-2022-27448"] | ["CWE-617"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | CVE-2018-2814 | ["CVE-2018-2814"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | NULL Pointer Dereference | ["CVE-2018-8740"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | NULL Pointer Dereference | ["CVE-2018-8740"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Integer Overflow or Wraparound | ["CVE-2022-22826"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| High | 400 | Integer Overflow or Wraparound | ["CVE-2022-42898"] | ["CWE-190"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| High | 400 | Integer Overflow or Wraparound | ["CVE-2022-23990"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 400 | Integer Overflow or Wraparound | ["CVE-2022-23990"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| High | 400 | Buffer Overflow | ["CVE-2020-12723"] | ["CWE-120"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Use of a Broken or Risky Cryptographic Algorithm | ["CVE-2020-25694"] | ["CWE-327"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Integer Overflow or Wraparound | ["CVE-2018-20847"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Out-of-bounds Write | ["CVE-2019-17546"] | ["CWE-787","CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Out-of-bounds Read | ["CVE-2018-16429"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 400 | Out-of-Bounds | ["CVE-2020-3898"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 400 | Out-of-Bounds | ["CVE-2020-3898"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| High | 400 | Improper Enforcement of Message or Data Structure | ["CVE-2020-11080"] | ["CWE-707"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| High | 400 | Improper Initialization | ["CVE-2020-11655"] | ["CWE-665"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | CVE-2018-3169 | ["CVE-2018-3169"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Incorrect Conversion between Numeric Types | ["CVE-2021-27218"] | ["CWE-681"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| High | 400 | Integer Overflow or Wraparound | ["CVE-2020-0198"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|--------------------|-----------------------|--|------------------|------------------|-------------------------|----------------|
| High | 400 | Key Management Errors | ["CVE-2018-0732"] | ["CWE-320"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Heap-based Buffer Overflow | ["CVE-2020-27814"] | ["CWE-122"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Out-of-bounds Read | ["CVE-2019-9936"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2022-27781"] | ["CWE-835"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| High | 400 | Integer Overflow or Wraparound | ["CVE-2017-16612"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Improper Input Validation | ["CVE-2017-11112"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| High | 400 | CVE-2020-2803 | ["CVE-2020-2803"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Out-of-bounds Read | ["CVE-2021-3712"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Cleartext Transmission of Sensitive Information | ["CVE-2022-43551"] | ["CWE-319"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| High | 400 | Cleartext Transmission of Sensitive Information | ["CVE-2022-43551"] | ["CWE-319"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| High | 400 | SQL Injection | ["CVE-2022-27381"] | ["CWE-89"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Double Free | ["CVE-2019-3829"] | ["CWE-415","CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| High | 400 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2022-27781"] | ["CWE-835"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 400 | Out-of-bounds Write | ["CVE-2018-25032"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | XML External Entity (XXE) Injection | ["CVE-2018-20843"] | ["CWE-611"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 400 | Out-of-bounds Write | ["CVE-2020-10543"] | ["CWE-787","CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Integer Overflow or Wraparound | ["CVE-2018-20346"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Use After Free | ["CVE-2022-27455"] | ["CWE-416"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Out-of-bounds Read | ["CVE-2018-10393"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| High | 400 | CVE-2022-21476 | ["CVE-2022-21476"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| High | 400 | Improper Certificate Validation | ["CVE-2019-17007"] | ["CWE-295"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| High | 400 | Out-of-bounds Write | ["CVE-2019-3856"] | ["CWE-787","CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| High | 400 | Improper Input Validation | ["CVE-2021-3580"] | ["CWE-20"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Out-of-Bounds | ["CVE-2017-2862"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 400 | Out-of-bounds Read | ["CVE-2018-10392"] | ["CWE-125","CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| High | 400 | Integer Overflow or Wraparound | ["CVE-2021-23840"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Integer Overflow or Wraparound | ["CVE-2022-22827"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 400 | Improper Privilege Management | ["CVE-2017-20002"] | ["CWE-269"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|--------------------|-----------------------|--|------------------|------------------|-------------------------|------------------|
| High | 400 | Reachable Assertion | ["CVE-2021-27212"] | ["CWE-617"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Use After Free | ["CVE-2020-13113"] | ["CWE-416"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Incorrect Calculation | ["CVE-2021-45960"] | ["CWE-682"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 400 | CVE-2017-9111 | ["CVE-2017-9111"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Use After Free | ["CVE-2020-13871"] | ["CWE-416"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Integer Overflow or Wraparound | ["CVE-2016-6328"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Integer Overflow or Wraparound | ["CVE-2020-10531"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| High | 400 | Use After Free | ["CVE-2019-18197"] | ["CWE-416","CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | NULL Pointer Dereference | ["CVE-2019-9937"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | CVE-2020-36226 | ["CVE-2020-36226"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Out-of-bounds Read | ["CVE-2018-19662"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| High | 400 | Out-of-bounds Write | ["CVE-2019-2201"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| High | 400 | Incorrect Conversion between Numeric Types | ["CVE-2021-27218"] | ["CWE-681"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 400 | Improper Certificate Validation | ["CVE-2022-27782"] | ["CWE-295"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| High | 400 | CVE-2017-9115 | ["CVE-2017-9115"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| High | 400 | Uncontrolled Recursion | ["CVE-2020-28196"] | ["CWE-674"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| High | 400 | Stack-based Buffer Overflow | ["CVE-2020-35492"] | ["CWE-121"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 400 | Stack-based Buffer Overflow | ["CVE-2020-35492"] | ["CWE-121"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| High | 400 | CVE-2017-10140 | ["CVE-2017-10140"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| High | 400 | Use After Free | ["CVE-2022-43680"] | ["CWE-416"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| High | 400 | Reachable Assertion | ["CVE-2020-36230"] | ["CWE-617"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| High | 400 | Improper Privilege Management | ["CVE-2017-20002"] | ["CWE-269"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 399 | Regular Expression Denial of Service (ReDoS) | ["CVE-2017-20162"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Low | 399 | Regular Expression Denial of Service (ReDoS) | ["CVE-2017-18214"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Low | 399 | Regular Expression Denial of Service (ReDoS) | ["CVE-2017-20162"] | ["CWE-400"] | e-corp-demo/container-breaking-in-goof(main):package.json | No Known Exploit | Auto Fixable | 2023-03-02 07:41:50.806 | Snyk Open Source |
| Low | 399 | Regular Expression Denial of Service (ReDoS) | ["CVE-2017-16138"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Low | 399 | Regular Expression Denial of Service (ReDoS) | ["CVE-2017-16138"] | ["CWE-400"] | e-corp-demo/container-breaking-in-goof(main):package.json | No Known Exploit | Auto Fixable | 2023-03-02 07:41:50.806 | Snyk Open Source |
| Low | 399 | Regular Expression Denial of Service (ReDoS) | ["CVE-2016-2515"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|--------------------|--------------|--|------------------|------------------|----------------------------|------------------|
| Medium | 387 | Prototype Pollution | ["CVE-2021-23807"] | ["CWE-1321"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 387 | Prototype Pollution | ["CVE-2021-23383"] | ["CWE-1321"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 375 | Denial of Service (DoS) | ["CVE-2019-20922"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 375 | Denial of Service (DoS) | ["CVE-2020-36518"] | ["CWE-400"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 375 | Regular Expression Denial of Service [] (ReDoS) | | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 375 | Allocation of Resources Without Limits or Throttling | ["CVE-2023-20863"] | ["CWE-770"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Not Auto Fixable | 2023-04-14 18:08:34.201 | Snyk Open Source |
| Medium | 372 | Regular Expression Denial of Service (ReDoS) | ["CVE-2021-23362"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Not Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 372 | Arbitrary File Upload | ["CVE-2022-27140"] | ["CWE-434"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Not Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 372 | Regular Expression Denial of Service (ReDoS) | ["CVE-2020-28469"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Not Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 372 | Arbitrary File Upload | ["CVE-2022-27261"] | ["CWE-434"] | e-corp-demo/goof-kubernetes(master):package.json | Proof of Concept | Not Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 371 | Out-of-bounds Write | ["CVE-2023-1906"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-04-13 21:35:31.166 | Snyk Container |
| Medium | 371 | LGPL-3.0 license | [] | [] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Data | Not Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| Medium | 371 | CDDL-1.0 license | [] | [] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Data | Not Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| Medium | 371 | CDDL-1.0 license | [] | [] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Data | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Medium | 371 | LGPL-2.0 license | [] | [] | e-corp-demo/java-goof(main):todolist-goof/todolist-core/pom.xml | No Data | Not Auto Fixable | 2023-03-07 21:11:13.069 | Snyk Open Source |
| Medium | 371 | LGPL-2.0 license | [] | [] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Data | Not Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| Medium | 371 | LGPL-2.0 license | [] | [] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Data | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Medium | 371 | LGPL-2.1 license | [] | [] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Data | Not Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| Medium | 371 | LGPL-2.1 license | [] | [] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Data | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Medium | 371 | LGPL-2.1 license | [] | [] | e-corp-demo/java-goof(main):todolist-goof/todolist-core/pom.xml | No Data | Not Auto Fixable | 2023-03-07 21:11:13.069 | Snyk Open Source |
| Medium | 371 | LGPL-3.0 license | [] | [] | e-corp-demo/java-goof(main):todolist-goof/todolist-core/pom.xml | No Data | Not Auto Fixable | 2023-03-07 21:11:13.069 | Snyk Open Source |
| Medium | 371 | EPL-1.0 license | [] | [] | e-corp-demo/java-goof(main):todolist-goof/todolist-core/pom.xml | No Data | Not Auto Fixable | 2023-03-07 21:11:13.069 | Snyk Open Source |
| Medium | 371 | LGPL-2.0 license | [] | [] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Data | Not Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| Medium | 371 | LGPL-2.0 license | [] | [] | e-corp-demo/java-goof(main):todolist-goof/todolist-core/pom.xml | No Data | Not Auto Fixable | 2023-03-07 21:11:13.069 | Snyk Open Source |
| Medium | 371 | LGPL-2.1 license | [] | [] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Data | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Medium | 371 | LGPL-3.0 license | [] | [] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Data | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Medium | 371 | LGPL-2.0 license | [] | [] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Data | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Medium | 371 | EPL-1.0 license | [] | [] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Data | Not Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|---|--------------------|--------------|--|------------------|------------------|----------------------------|------------------|
| Medium | 371 | LGPL-2.1 license | [] | [] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Data | Not Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| Medium | 371 | EPL-1.0 license | [] | [] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Data | Not Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| Medium | 371 | Improper Input Validation | ["CVE-2023-27043"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-04-21 08:24:56.421 | Snyk Container |
| Medium | 371 | EPL-1.0 license | [] | [] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Data | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Medium | 371 | EPL-1.0 license | [] | [] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Data | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Medium | 371 | EPL-1.0 license | [] | [] | e-corp-demo/java-goof(main):todolist-goof/todolist-core/pom.xml | No Data | Not Auto Fixable | 2023-03-07 21:11:13.069 | Snyk Open Source |
| High | 370 | XML External Entity (XXE) Injection | ["CVE-2020-10683"] | ["CWE-611"] | e-corp-demo/java-goof(main):todolist-goof/todolist-core/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:13.069 | Snyk Open Source |
| High | 370 | XML External Entity (XXE) Injection | ["CVE-2020-10683"] | ["CWE-611"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| Medium | 370 | Denial of Service (DoS) | ["CVE-2022-42004"] | ["CWE-400"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Proof of Concept | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Medium | 370 | Denial of Service (DoS) | ["CVE-2022-42003"] | ["CWE-400"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | Proof of Concept | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 370 | XML External Entity (XXE) Injection | ["CVE-2020-10683"] | ["CWE-611"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 365 | XML External Entity (XXE) Injection | ["CVE-2015-0254"] | ["CWE-94"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| High | 365 | XML External Entity (XXE) Injection | ["CVE-2015-0254"] | ["CWE-94"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Medium | 365 | Improper Input Validation | ["CVE-2021-22060"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| High | 365 | Prototype Pollution | ["CVE-2019-19919"] | ["CWE-1321"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 365 | Improper Output Neutralization for Logs | ["CVE-2021-22096"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/todolist-core/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:13.069 | Snyk Open Source |
| High | 365 | Prototype Pollution | [] | ["CWE-1321"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| High | 365 | Prototype Pollution | [] | ["CWE-1321"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 365 | Improper Input Validation | ["CVE-2021-22060"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/todolist-core/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:13.069 | Snyk Open Source |
| Medium | 365 | Improper Output Neutralization for Logs | ["CVE-2021-22096"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Low | 364 | Integer Overflow or Wraparound | ["CVE-2020-27764"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 364 | Improper Input Validation | ["CVE-2019-20907"] | ["CWE-20"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 364 | Missing Initialization of Resource | ["CVE-2021-22898"] | ["CWE-909"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 364 | Missing Initialization of Resource | ["CVE-2021-22898"] | ["CWE-909"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 364 | Integer Overflow or Wraparound | ["CVE-2020-27771"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 364 | Out-of-bounds Write | ["CVE-2019-19948"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 364 | Divide By Zero | ["CVE-2020-27763"] | ["CWE-369"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 364 | Use of Incorrectly-Resolved Name or Reference | ["CVE-2021-22924"] | ["CWE-706"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|--------------------|------------------------|--|------------------|------------------|-------------------------|------------------|
| Low | 364 | Integer Overflow or Wraparound | ["CVE-2020-27751"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 364 | Use of Incorrectly-Resolved Name or Reference | ["CVE-2021-22924"] | ["CWE-706"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 364 | Missing Initialization of Resource | ["CVE-2021-22898"] | ["CWE-909"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 364 | Use of Incorrectly-Resolved Name or Reference | ["CVE-2021-22924"] | ["CWE-706"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 364 | Divide By Zero | ["CVE-2020-27560"] | ["CWE-369"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 364 | Integer Overflow or Wraparound | ["CVE-2020-27759"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 364 | Integer Overflow or Wraparound | ["CVE-2020-27768"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 364 | Resource Exhaustion | ["CVE-2019-13232"] | ["CWE-400"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 364 | Integer Overflow or Wraparound | ["CVE-2020-25666"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 364 | Integer Overflow or Wraparound | ["CVE-2020-27772"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 364 | Integer Overflow or Wraparound | ["CVE-2020-27761"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 364 | Divide By Zero | ["CVE-2020-27773"] | ["CWE-369"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 364 | Integer Overflow or Wraparound | ["CVE-2020-25675"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 364 | Integer Overflow or Wraparound | ["CVE-2020-27758"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 364 | CVE-2022-35252 | ["CVE-2022-35252"] | [] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 364 | Use of a Broken or Risky Cryptographic Algorithm | ["CVE-2019-1563"] | ["CWE-327", "CWE-339"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 364 | CVE-2020-8284 | ["CVE-2020-8284"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 364 | CVE-2020-8284 | ["CVE-2020-8284"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 364 | Integer Overflow or Wraparound | ["CVE-2020-27775"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 364 | Integer Overflow or Wraparound | ["CVE-2020-27767"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 364 | Integer Overflow or Wraparound | ["CVE-2020-27757"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 364 | Integer Overflow or Wraparound | ["CVE-2020-27754"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 364 | Integer Overflow or Wraparound | ["CVE-2020-27769"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 364 | Integer Overflow or Wraparound | ["CVE-2020-27776"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 364 | Divide By Zero | ["CVE-2020-27765"] | ["CWE-369"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 364 | Integer Overflow or Wraparound | ["CVE-2020-27774"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 335 | Man-in-the-Middle (MitM) | ["CVE-2020-9488"] | ["CWE-297"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Medium | 333 | Cross-site Scripting (XSS) | ["CVE-2019-10219"] | ["CWE-79"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|----------------------|-------------|--|------------------|------------------|----------------------------|------------------|
| Low | 321 | Out-of-bounds Read | ["CVE-2017-14939"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | Mature | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 321 | Integer Overflow or Wraparound | ["CVE-2018-6323"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | Mature | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 321 | Improper Check for Dropped Privileges | ["CVE-2019-18276"] | ["CWE-273"] | e-corp-demo/goof-kubernetes(master):Dockerfile | Mature | Not Auto Fixable | 2023-03-07 23:04:19.449 | Snyk Container |
| Low | 321 | Improper Check for Dropped Privileges | ["CVE-2019-18276"] | ["CWE-273"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | Mature | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 321 | OS Command Injection | ["CVE-2019-9193"] | ["CWE-78"] | e-corp-demo/goof-kubernetes(master):Dockerfile | Mature | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 321 | Inappropriate Encoding for Output Context | ["CVE-2019-6110"] | ["CWE-838"] | e-corp-demo/goof-kubernetes(master):Dockerfile | Mature | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 321 | Out-of-bounds Write | ["CVE-2018-1000001"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | Mature | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 321 | Out-of-bounds Write | ["CVE-2018-1000001"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | Mature | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 321 | Inappropriate Encoding for Output Context | ["CVE-2019-6110"] | ["CWE-838"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | Mature | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 321 | Out-of-Bounds | ["CVE-2017-8834"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | Mature | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 321 | Out-of-Bounds | ["CVE-2017-8834"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | Mature | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 321 | Inappropriate Encoding for Output Context | ["CVE-2019-6110"] | ["CWE-838"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | Mature | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Medium | 310 | Regular Expression Denial of Service (ReDoS) | ["CVE-2017-18077"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 300 | Out-of-bounds Read | ["CVE-2020-27845"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Integer Overflow or Wraparound | ["CVE-2021-29338"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Use of a Broken or Risky Cryptographic Algorithm | ["CVE-2018-10844"] | ["CWE-327"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Medium | 300 | HTTP Request Smuggling | ["CVE-2022-32213"] | ["CWE-444"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.457 | Snyk Container |
| Medium | 300 | CVE-2018-2677 | ["CVE-2018-2677"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Improper Resource Shutdown or Release | ["CVE-2020-12049"] | ["CWE-404"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Medium | 300 | CVE-2019-2949 | ["CVE-2019-2949"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Reachable Assertion | ["CVE-2018-20217"] | ["CWE-617"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.455 | Snyk Container |
| Medium | 300 | Heap-based Buffer Overflow | ["CVE-2020-27841"] | ["CWE-122"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Improper Locking | ["CVE-2022-31623"] | ["CWE-667"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Information Exposure | ["CVE-2017-3738"] | ["CWE-200"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | CVE-2017-10357 | ["CVE-2017-10357"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | NULL Pointer Dereference | ["CVE-2018-10196"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 300 | Out-of-bounds Read | ["CVE-2019-2228"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Medium | 300 | Improper Certificate Validation | ["CVE-2022-22747"] | ["CWE-295"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|--------------------|-----------------------|--|------------------|------------------|-------------------------|----------------|
| Medium | 300 | Out-of-bounds Write | ["CVE-2022-0529"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Use of a Broken or Risky Cryptographic Algorithm | ["CVE-2020-12402"] | ["CWE-327"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | Improper Input Validation | ["CVE-2017-11613"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | NULL Pointer Dereference | ["CVE-2021-37750"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.455 | Snyk Container |
| Medium | 300 | Out-of-bounds Read | ["CVE-2018-16062"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Medium | 300 | Integer Overflow or Wraparound | ["CVE-2017-15422"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Medium | 300 | Out-of-bounds Read | ["CVE-2020-11762"] | ["CWE-125","CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Information Exposure | ["CVE-2021-32028"] | ["CWE-200"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Buffer Overflow | ["CVE-2020-8252"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.457 | Snyk Container |
| Medium | 300 | CVE-2020-14556 | ["CVE-2020-14556"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Improper Certificate Validation | ["CVE-2019-11727"] | ["CWE-295"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | Insufficiently Protected Credentials | ["CVE-2022-27776"] | ["CWE-522"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Medium | 300 | Insufficiently Protected Credentials | ["CVE-2022-27776"] | ["CWE-522"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Medium | 300 | Information Exposure | ["CVE-2020-12399"] | ["CWE-203"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | Out-of-Bounds | ["CVE-2017-13734"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | CVE-2019-13057 | ["CVE-2019-13057"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | CVE-2017-9116 | ["CVE-2017-9116"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | CVE-2020-14765 | ["CVE-2020-14765"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Improper Resource Shutdown or Release | ["CVE-2022-31624"] | ["CWE-404"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | NULL Pointer Dereference | ["CVE-2018-19217"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | Use After Free | ["CVE-2020-15305"] | ["CWE-416"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | CVE-2017-10281 | ["CVE-2017-10281"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | CVE-2017-9114 | ["CVE-2017-9114"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Out-of-bounds Read | ["CVE-2019-7665"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Medium | 300 | Out-of-bounds Read | ["CVE-2019-15145"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Medium | 300 | CVE-2018-4181 | ["CVE-2018-4181"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Medium | 300 | Divide By Zero | ["CVE-2022-2057"] | ["CWE-369"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Cleartext Transmission of Sensitive Information | ["CVE-2023-23915"] | ["CWE-319"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|--------------------|-------------|--|------------------|------------------|-------------------------|----------------|
| Medium | 300 | NULL Pointer Dereference | ["CVE-2020-13632"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | CVE-2019-2975 | ["CVE-2019-2975"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Allocation of Resources Without Limits or Throttling | ["CVE-2022-32206"] | ["CWE-770"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Medium | 300 | CVE-2020-2812 | ["CVE-2020-2812"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Out-of-Bounds | ["CVE-2017-13733"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | CVE-2022-21496 | ["CVE-2022-21496"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | CVE-2017-9112 | ["CVE-2017-9112"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Improper Handling of URL Encoding | ["CVE-2021-44531"] | ["CWE-177"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.457 | Snyk Container |
| Medium | 300 | Improper Input Validation | ["CVE-2017-18248"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Medium | 300 | CVE-2018-2641 | ["CVE-2018-2641"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | Out-of-bounds Read | ["CVE-2020-11760"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Reachable Assertion | ["CVE-2022-0865"] | ["CWE-617"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | CVE-2018-2797 | ["CVE-2018-2797"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | CVE-2022-21426 | ["CVE-2022-21426"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | NULL Pointer Dereference | ["CVE-2021-3449"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.457 | Snyk Container |
| Medium | 300 | CVE-2018-2800 | ["CVE-2018-2800"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | Reachable Assertion | ["CVE-2017-11368"] | ["CWE-617"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Medium | 300 | Divide By Zero | ["CVE-2019-16168"] | ["CWE-369"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Integer Overflow or Wraparound | ["CVE-2021-23841"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Out-of-bounds Read | ["CVE-2022-1354"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | CVE-2020-2574 | ["CVE-2020-2574"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | CVE-2018-2798 | ["CVE-2018-2798"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | Out-of-bounds Read | ["CVE-2020-29362"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | NULL Pointer Dereference | ["CVE-2018-17000"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | CVE-2020-14803 | ["CVE-2020-14803"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | Out-of-Bounds | ["CVE-2017-3735"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | CVE-2022-21360 | ["CVE-2022-21360"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | CVE-2018-3214 | ["CVE-2018-3214"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|--------------------|----------------------------------|--|------------------|------------------|-------------------------|----------------|
| Medium | 300 | CVE-2022-21365 | ["CVE-2022-21365"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | CVE-2021-2369 | ["CVE-2021-2369"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | Out-of-bounds Read | ["CVE-2020-0093"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Divide By Zero | ["CVE-2022-2058"] | ["CWE-369"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Uncontrolled Recursion | ["CVE-2019-15144"] | ["CWE-674"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Medium | 300 | Integer Overflow or Wraparound | ["CVE-2021-23841"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2021-3468"] | ["CWE-835"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Medium | 300 | Out-of-bounds Read | ["CVE-2020-11761"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | CVE-2019-2762 | ["CVE-2019-2762"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | CVE-2020-2601 | ["CVE-2020-2601"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Out-of-bounds Write | ["CVE-2020-11764"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Reachable Assertion | ["CVE-2017-13726"] | ["CWE-617"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | CVE-2022-21294 | ["CVE-2022-21294"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | CVE-2022-21282 | ["CVE-2022-21282"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | Resource Exhaustion | ["CVE-2021-3479"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Out-of-bounds Write | ["CVE-2020-19144"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | CVE-2021-35578 | ["CVE-2021-35578"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | Insufficiently Protected Credentials | ["CVE-2022-27774"] | ["CWE-522"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Medium | 300 | Out-of-bounds Read | ["CVE-2019-7150"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Medium | 300 | CVE-2018-2815 | ["CVE-2018-2815"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | CVE-2020-2800 | ["CVE-2020-2800"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Out-of-bounds Read | ["CVE-2018-19661"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Medium | 300 | Out-of-Bounds | ["CVE-2018-18520"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Medium | 300 | Insufficiently Protected Credentials | ["CVE-2021-23222"] | ["CWE-522"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Improper Input Validation | ["CVE-2020-27824"] | ["CWE-20", "CWE-125", "CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Integer Overflow or Wraparound | ["CVE-2021-20300"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | CVE-2022-21305 | ["CVE-2022-21305"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|--------------------|-----------------------|--|------------------|------------------|-------------------------|----------------|
| Medium | 300 | Use of a Broken or Risky Cryptographic Algorithm | ["CVE-2018-0737"] | ["CWE-327"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | NULL Pointer Dereference | ["CVE-2022-0561"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | CVE-2017-10350 | ["CVE-2017-10350"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | CVE-2021-35550 | ["CVE-2021-35550"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2019-15143"] | ["CWE-835"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Medium | 300 | CVE-2019-2745 | ["CVE-2019-2745"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | HTTP Request Smuggling | ["CVE-2022-32215"] | ["CWE-444"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.457 | Snyk Container |
| Medium | 300 | HTTP Request Smuggling | ["CVE-2022-32214"] | ["CWE-444"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.457 | Snyk Container |
| Medium | 300 | CVE-2018-2629 | ["CVE-2018-2629"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | CVE-2019-2974 | ["CVE-2019-2974"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | CVE-2020-2593 | ["CVE-2020-2593"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | CVE-2018-2799 | ["CVE-2018-2799"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | Out-of-bounds Read | ["CVE-2020-0499"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Medium | 300 | Improper Certificate Validation | ["CVE-2021-44533"] | ["CWE-295"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.457 | Snyk Container |
| Medium | 300 | CVE-2018-3180 | ["CVE-2018-3180"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Use After Free | ["CVE-2019-7317"] | ["CWE-416"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Medium | 300 | Integer Overflow or Wraparound | ["CVE-2021-23215"] | ["CWE-190"; "CWE-59"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Link Following | ["CVE-2021-28153"] | ["CWE-59"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Medium | 300 | Out-of-bounds Read | ["CVE-2020-27842"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Out-of-bounds Read | ["CVE-2022-1623"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Divide By Zero | ["CVE-2018-18521"] | ["CWE-369"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Medium | 300 | Integer Overflow or Wraparound | ["CVE-2020-13434"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | NULL Pointer Dereference | ["CVE-2020-1971"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | CVE-2021-35556 | ["CVE-2021-35556"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | Allocation of Resources Without Limits or Throttling | ["CVE-2022-32206"] | ["CWE-770"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Medium | 300 | Out-of-bounds Read | ["CVE-2020-27843"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | CVE-2020-6829 | ["CVE-2020-6829"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | CVE-2020-2814 | ["CVE-2020-2814"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|--------------------|-----------------------|--|------------------|------------------|-------------------------|----------------|
| Medium | 300 | Reachable Assertion | ["CVE-2018-20217"] | ["CWE-617"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Medium | 300 | CVE-2018-2602 | ["CVE-2018-2602"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | CVE-2021-35559 | ["CVE-2021-35559"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | CVE-2020-14792 | ["CVE-2020-14792"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | Out-of-bounds Read | ["CVE-2021-3477"] | ["CWE-125","CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Out-of-bounds Read | ["CVE-2021-3605"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Out-of-bounds Read | ["CVE-2019-2228"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Medium | 300 | Reachable Assertion | ["CVE-2017-13727"] | ["CWE-617"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | CVE-2020-14812 | ["CVE-2020-14812"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Resource Exhaustion | ["CVE-2019-20446"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Resource Exhaustion | ["CVE-2019-20446"] | ["CWE-400"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Medium | 300 | Use After Free | ["CVE-2017-12133"] | ["CWE-416"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Medium | 300 | HTTP Request Smuggling | ["CVE-2021-22959"] | ["CWE-444"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.457 | Snyk Container |
| Medium | 300 | NULL Pointer Dereference | ["CVE-2022-0561"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Resource Exhaustion | ["CVE-2022-1210"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Resource Exhaustion | ["CVE-2022-1210"] | ["CWE-400"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-6888"] | ["CWE-772"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Medium | 300 | Out-of-bounds Write | ["CVE-2020-28241"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | CVE-2019-2989 | ["CVE-2019-2989"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Allocation of Resources Without Limits or Throttling | ["CVE-2021-33910"] | ["CWE-770"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Use After Free | ["CVE-2020-21913"] | ["CWE-416"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 300 | Use After Free | ["CVE-2020-21913"] | ["CWE-416"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Medium | 300 | Resource Exhaustion | ["CVE-2021-3478"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Out-of-bounds Read | ["CVE-2022-1622"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | DNS Rebinding | ["CVE-2022-32212"] | ["CWE-350"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.457 | Snyk Container |
| Medium | 300 | NULL Pointer Dereference | ["CVE-2018-19210"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | CVE-2022-0530 | ["CVE-2022-0530"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | CVE-2022-0530 | ["CVE-2022-0530"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.457 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|---|--------------------|-------------|--|------------------|------------------|-------------------------|----------------|
| Medium | 300 | Out-of-bounds Write | ["CVE-2020-16589"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | CVE-2022-21349 | ["CVE-2022-21349"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | CVE-2019-7663 | ["CVE-2019-7663"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Uncontrolled Recursion | ["CVE-2018-0739"] | ["CWE-674"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | CVE-2021-35586 | ["CVE-2021-35586"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | CVE-2021-35567 | ["CVE-2021-35567"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | CVE-2020-14621 | ["CVE-2020-14621"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | CVE-2018-2588 | ["CVE-2018-2588"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Out-of-bounds Read | ["CVE-2018-14498"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Medium | 300 | Out-of-bounds Read | ["CVE-2018-14498"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Out-of-bounds Read | ["CVE-2017-14633"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Medium | 300 | Information Exposure | ["CVE-2019-1551"] | ["CWE-200"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Out-of-bounds Write | ["CVE-2020-15306"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Information Exposure | ["CVE-2019-1559"] | ["CWE-203"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | CVE-2021-20302 | ["CVE-2021-20302"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Improper Input Validation | ["CVE-2021-22939"] | ["CWE-20"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.457 | Snyk Container |
| Medium | 300 | Out-of-bounds Read | ["CVE-2019-7665"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Medium | 300 | CVE-2021-35564 | ["CVE-2021-35564"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | Resource Exhaustion | ["CVE-2022-25313"] | ["CWE-400"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Medium | 300 | Resource Exhaustion | ["CVE-2022-25313"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Medium | 300 | CVE-2018-2796 | ["CVE-2018-2796"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Integer Overflow or Wraparound | ["CVE-2021-3474"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | CVE-2021-35561 | ["CVE-2021-35561"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | Improper Locking | ["CVE-2022-31621"] | ["CWE-667"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | NULL Pointer Dereference | ["CVE-2020-16588"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Out-of-bounds Write | ["CVE-2021-0561"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Medium | 300 | NULL Pointer Dereference | ["CVE-2020-13632"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Cleartext Transmission of Sensitive Information | ["CVE-2023-23915"] | ["CWE-319"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--------------------------------|--------------------|-------------|--|------------------|------------------|-------------------------|----------------|
| Medium | 300 | Arbitrary Code Injection | ["CVE-2022-34903"] | ["CWE-74"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Medium | 300 | Arbitrary Code Injection | ["CVE-2022-34903"] | ["CWE-74"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Medium | 300 | Divide By Zero | ["CVE-2022-2057"] | ["CWE-369"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Out-of-bounds Write | ["CVE-2020-16587"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Divide By Zero | ["CVE-2022-0909"] | ["CWE-369"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Divide By Zero | ["CVE-2022-2056"] | ["CWE-369"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Divide By Zero | ["CVE-2022-2056"] | ["CWE-369"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Out-of-bounds Read | ["CVE-2019-2180"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Medium | 300 | Use After Free | ["CVE-2020-15389"] | ["CWE-416"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Out-of-bounds Read | ["CVE-2020-0182"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Out-of-bounds Read | ["CVE-2019-3832"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Medium | 300 | Out-of-bounds Read | ["CVE-2018-16062"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Medium | 300 | NULL Pointer Dereference | ["CVE-2021-37750"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Medium | 300 | CVE-2019-1547 | ["CVE-2019-1547"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Integer Overflow or Wraparound | ["CVE-2017-6312"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Medium | 300 | CVE-2022-21434 | ["CVE-2022-21434"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | Out-of-bounds Write | ["CVE-2022-0529"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.457 | Snyk Container |
| Medium | 300 | NULL Pointer Dereference | ["CVE-2018-5729"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.455 | Snyk Container |
| Medium | 300 | Divide By Zero | ["CVE-2020-12767"] | ["CWE-369"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | NULL Pointer Dereference | ["CVE-2022-0908"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | NULL Pointer Dereference | ["CVE-2022-0908"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Reachable Assertion | ["CVE-2022-0865"] | ["CWE-617"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | CVE-2018-2582 | ["CVE-2018-2582"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | CVE-2021-2022 | ["CVE-2021-2022"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Out-of-bounds Write | ["CVE-2021-3630"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Medium | 300 | CVE-2017-10274 | ["CVE-2017-10274"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | Out-of-bounds Read | ["CVE-2019-7150"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Medium | 300 | Out-of-Bounds | ["CVE-2018-18520"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|--------------------|-----------------------|--|------------------|------------------|-------------------------|----------------|
| Medium | 300 | Insufficiently Protected Credentials | ["CVE-2022-27774"] | ["CWE-522"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Medium | 300 | Integer Overflow or Wraparound | ["CVE-2020-14344"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Medium | 300 | Integer Overflow or Wraparound | ["CVE-2020-14344"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Out-of-bounds Read | ["CVE-2022-0924"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | CVE-2018-2599 | ["CVE-2018-2599"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Use After Free | ["CVE-2020-8265"] | ["CWE-416"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.457 | Snyk Container |
| Medium | 300 | Information Exposure | ["CVE-2017-10356"] | ["CWE-200"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2021-3468"] | ["CWE-835"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.449 | Snyk Container |
| Medium | 300 | Out-of-Bounds | ["CVE-2018-18310"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Medium | 300 | DLL Hijacking | ["CVE-2022-32223"] | ["CWE-427"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.457 | Snyk Container |
| Medium | 300 | Out-of-bounds Read | ["CVE-2020-11758"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Out-of-bounds Write | ["CVE-2021-46822"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Medium | 300 | Out-of-bounds Write | ["CVE-2021-46822"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Integer Overflow or Wraparound | ["CVE-2019-14973"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Integer Overflow or Wraparound | ["CVE-2019-14973"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Divide By Zero | ["CVE-2022-2058"] | ["CWE-369"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Off-by-one Error | ["CVE-2020-11765"] | ["CWE-193"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Out-of-bounds Write | ["CVE-2022-32208"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Medium | 300 | Resource Exhaustion | ["CVE-2018-5784"] | ["CWE-400"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Divide By Zero | ["CVE-2018-1152"] | ["CWE-369"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Medium | 300 | CVE-2018-2634 | ["CVE-2018-2634"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Out-of-bounds Write | ["CVE-2018-16435"] | ["CWE-787","CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Medium | 300 | NULL Pointer Dereference | ["CVE-2022-0562"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | NULL Pointer Dereference | ["CVE-2022-0562"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Out-of-bounds Read | ["CVE-2022-22844"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Out-of-bounds Read | ["CVE-2022-22844"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | NULL Pointer Dereference | ["CVE-2017-18013"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Information Exposure | ["CVE-2022-2097"] | ["CWE-200"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.457 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|--------------------|-----------------------|--|------------------|------------------|-------------------------|----------------|
| Medium | 300 | Integer Overflow or Wraparound | ["CVE-2021-3475"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | CVE-2019-2816 | ["CVE-2019-2816"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Out-of-Bounds | ["CVE-2017-13732"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | CVE-2020-2752 | ["CVE-2020-2752"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | CVE-2020-2781 | ["CVE-2020-2781"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Integer Overflow or Wraparound | ["CVE-2021-20303"] | ["CWE-190","CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Improper Certificate Validation | ["CVE-2020-13645"] | ["CWE-295"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Medium | 300 | Improper Resource Shutdown or Release | ["CVE-2022-31622"] | ["CWE-404"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Integer Overflow or Wraparound | ["CVE-2020-11759"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Use of a Broken or Risky Cryptographic Algorithm | ["CVE-2018-10845"] | ["CWE-327"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Medium | 300 | CVE-2018-12404 | ["CVE-2018-12404"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | Out-of-Bounds | ["CVE-2018-18310"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Medium | 300 | Out-of-bounds Read | ["CVE-2017-3737"] | ["CWE-125","CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | NULL Pointer Dereference | ["CVE-2021-20296"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Out-of-bounds Read | ["CVE-2018-19758"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Medium | 300 | NULL Pointer Dereference | ["CVE-2018-18508"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | NULL Pointer Dereference | ["CVE-2020-1971"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2017-6314"] | ["CWE-835"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Medium | 300 | Improper Privilege Management | ["CVE-2022-26691"] | ["CWE-269"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Medium | 300 | Improper Privilege Management | ["CVE-2022-26691"] | ["CWE-269"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Medium | 300 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-15671"] | ["CWE-772"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Medium | 300 | CVE-2022-21340 | ["CVE-2022-21340"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | CVE-2021-35565 | ["CVE-2021-35565"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | Out-of-bounds Read | ["CVE-2022-1354"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Out-of-Bounds | ["CVE-2017-13729"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | Information Exposure | ["CVE-2018-4300"] | ["CWE-200"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Medium | 300 | CVE-2018-2678 | ["CVE-2018-2678"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | Information Exposure | ["CVE-2020-12400"] | ["CWE-200"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|-------------------------------------|------------------------|--|------------------|------------------|-------------------------|----------------|
| Medium | 300 | CVE-2021-2163 | ["CVE-2021-2163"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | Link Following | ["CVE-2021-28153"] | ["CWE-59"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Medium | 300 | CVE-2022-21341 | ["CVE-2022-21341"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | CVE-2017-10347 | ["CVE-2017-10347"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | CVE-2020-2830 | ["CVE-2020-2830"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | CVE-2021-4160 | ["CVE-2021-4160"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Improper Input Validation | ["CVE-2020-10001"] | ["CWE-20"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Medium | 300 | Excessive Iteration | ["CVE-2019-12973"] | ["CWE-834"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | CVE-2018-2795 | ["CVE-2018-2795"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | NULL Pointer Dereference | ["CVE-2022-0907"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | NULL Pointer Dereference | ["CVE-2022-0907"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Race Condition | ["CVE-2018-1049"] | ["CWE-362"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Out-of-bounds Read | ["CVE-2022-1623"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Divide By Zero | ["CVE-2018-18521"] | ["CWE-369"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Medium | 300 | Out-of-bounds Read | ["CVE-2020-11763"] | ["CWE-125", "CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | CVE-2021-4160 | ["CVE-2021-4160"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | CVE-2019-2999 | ["CVE-2019-2999"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Out-of-Bounds | ["CVE-2021-3598"] | ["CWE-119", "CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | NULL Pointer Dereference | ["CVE-2018-17000"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | CVE-2017-10348 | ["CVE-2017-10348"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | CVE-2022-21296 | ["CVE-2022-21296"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | CVE-2017-9110 | ["CVE-2017-9110"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Out-of-bounds Read | ["CVE-2020-29362"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | CVE-2018-2618 | ["CVE-2018-2618"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | Divide By Zero | ["CVE-2017-14634"] | ["CWE-369"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Medium | 300 | Integer Underflow | ["CVE-2021-26260"] | ["CWE-191", "CWE-191"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Use of a Broken or Risky Cryptographic Algorithm | ["CVE-2018-0734"] | ["CWE-327"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Improper Input Validation | ["CVE-2021-22931", "CVE-2021-3672"] | ["CWE-20"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.457 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|--------------------|-------------------|--|------------------|------------------|-------------------------|----------------|
| Medium | 300 | Out-of-bounds Read | ["CVE-2019-15142"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Medium | 300 | Out-of-Bounds | ["CVE-2019-6454"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | CVE-2019-2684 | ["CVE-2019-2684"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | Integer Overflow or Wraparound | ["CVE-2021-3476"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Out-of-bounds Read | ["CVE-2022-1622"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | CVE-2018-2603 | ["CVE-2018-2603"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | NULL Pointer Dereference | ["CVE-2018-19210"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | CVE-2022-21283 | ["CVE-2022-21283"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | NULL Pointer Dereference | ["CVE-2018-5729"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Medium | 300 | CVE-2019-7663 | ["CVE-2019-7663"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Divide By Zero | ["CVE-2022-0909"] | ["CWE-369"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Integer Overflow or Wraparound | ["CVE-2020-13434"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Use of a Broken or Risky Cryptographic Algorithm | ["CVE-2018-10846"] | ["CWE-327"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Medium | 300 | Out-of-Bounds | ["CVE-2017-13730"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | Out-of-Bounds | ["CVE-2017-13731"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | CVE-2017-10349 | ["CVE-2017-10349"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | Allocation of Resources Without Limits or Throttling | ["CVE-2021-33910"] | ["CWE-770"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Improper Initialization | ["CVE-2022-1122"] | ["CWE-665","CWE-" | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | CVE-2019-2769 | ["CVE-2019-2769"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Use of a Broken or Risky Cryptographic Algorithm | ["CVE-2020-12401"] | ["CWE-327"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | CVE-2018-2663 | ["CVE-2018-2663"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | Missing Authorization | ["CVE-2020-1720"] | ["CWE-862"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | CVE-2017-10295 | ["CVE-2017-10295"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | NULL Pointer Dereference | ["CVE-2018-7456"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Stack-based Buffer Overflow | ["CVE-2022-1355"] | ["CWE-121"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Out-of-bounds Write | ["CVE-2022-32208"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Medium | 300 | Improper Input Validation | ["CVE-2020-10001"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Medium | 300 | Improper Certificate Validation | ["CVE-2021-44532"] | ["CWE-295"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.457 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|--------------------|--------------|---|------------------|------------------|-------------------------|------------------|
| Medium | 300 | CVE-2022-21293 | ["CVE-2022-21293"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | Divide By Zero | ["CVE-2019-16168"] | ["CWE-369"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | CVE-2022-21299 | ["CVE-2022-21299"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Medium | 300 | Stack-based Buffer Overflow | ["CVE-2022-1355"] | ["CWE-121"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | HTTP Request Smuggling | ["CVE-2021-22960"] | ["CWE-444"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.457 | Snyk Container |
| Medium | 300 | Divide By Zero | ["CVE-2018-1152"] | ["CWE-369"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Out-of-bounds Read | ["CVE-2022-0924"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 300 | Out-of-bounds Write | ["CVE-2020-19144"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Medium | 300 | Information Exposure | ["CVE-2017-3736"] | ["CWE-200"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Medium | 265 | Denial of Service (DoS) | ["CVE-2022-22950"] | ["CWE-400"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| Medium | 265 | Denial of Service (DoS) | ["CVE-2022-1259"] | ["CWE-400"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-12 18:46:04.451 | Snyk Open Source |
| Medium | 265 | Denial of Service (DoS) | [] | ["CWE-399"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Medium | 265 | Regular Expression Denial of Service (ReDoS) | [] | ["CWE-1333"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Medium | 265 | JSM bypass via ReflectionHelper | ["CVE-2014-3558"] | ["CWE-592"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Medium | 265 | Denial of Service (DoS) | [] | ["CWE-399"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Medium | 265 | Directory Traversal | ["CVE-2014-3578"] | ["CWE-22"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| Medium | 265 | Denial of Service (DoS) | ["CVE-2022-22970"] | ["CWE-400"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| Medium | 265 | Allocation of Resources Without Limits or Throttling | ["CVE-2023-20861"] | ["CWE-770"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-24 01:21:57.413 | Snyk Open Source |
| Medium | 265 | Improper Input Validation | ["CVE-2020-10693"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-struts/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:36.276 | Snyk Open Source |
| Medium | 265 | Regular Expression Denial of Service (ReDoS) | ["CVE-2022-3517"] | ["CWE-1333"] | e-corp-demo/goof-kubernetes(master):package.json | No Known Exploit | Auto Fixable | 2023-03-07 23:04:09.540 | Snyk Open Source |
| Low | 260 | Improper Handling of Case Sensitivity | ["CVE-2022-22968"] | ["CWE-178"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | Proof of Concept | Not Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| Low | 250 | Container is running with writable root filesystem | [] | [] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/k8s/deploy.yaml | | Not Auto Fixable | 2023-03-07 21:11:03.946 | Snyk IaC |
| Low | 250 | Container is running without liveness probe | [] | [] | e-corp-demo/goof-kubernetes(master):goof-mongo-deployment.yaml | | Not Auto Fixable | 2023-03-07 23:04:06.675 | Snyk IaC |
| Low | 250 | Container is running without liveness probe | [] | [] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/k8s/deploy.yaml | | Not Auto Fixable | 2023-03-07 21:11:03.946 | Snyk IaC |
| Low | 250 | Container is running without liveness probe | [] | [] | e-corp-demo/goof-kubernetes(master):goof-deployment.yaml | | Not Auto Fixable | 2023-03-07 23:04:06.635 | Snyk IaC |
| Low | 250 | Container's UID could clash with host's UID | [] | [] | e-corp-demo/goof-kubernetes(master):goof-deployment.yaml | | Not Auto Fixable | 2023-03-14 19:02:16.784 | Snyk IaC |
| Low | 250 | Container's UID could clash with host's UID | [] | [] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/k8s/deploy.yaml | | Not Auto Fixable | 2023-03-15 22:03:28.481 | Snyk IaC |
| Low | 250 | Container is running without memory limit | [] | [] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/k8s/deploy.yaml | | Not Auto Fixable | 2023-03-07 21:11:03.946 | Snyk IaC |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|--------------------|-----------------------|---|------------------|------------------|----------------------------|------------------|
| Low | 250 | Container has no CPU limit | [] | [] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/k8s/deploy.yaml | | Not Auto Fixable | 2023-03-07 21:11:03.946 | Snyk IaC |
| Low | 250 | Container has no CPU limit | [] | [] | e-corp-demo/goof-kubernetes(master):goof-deployment.yaml | | Not Auto Fixable | 2023-03-07 23:04:06.635 | Snyk IaC |
| Low | 250 | Container is running without memory limit | [] | [] | e-corp-demo/goof-kubernetes(master):goof-mongo-deployment.yaml | | Not Auto Fixable | 2023-03-07 23:04:06.675 | Snyk IaC |
| Low | 250 | Container is running with writable root filesystem | [] | [] | e-corp-demo/goof-kubernetes(master):goof-deployment.yaml | | Not Auto Fixable | 2023-03-07 23:04:06.635 | Snyk IaC |
| Low | 250 | Container could be running with outdated image | [] | [] | e-corp-demo/goof-kubernetes(master):goof-mongo-deployment.yaml | | Not Auto Fixable | 2023-03-07 23:04:06.675 | Snyk IaC |
| Low | 250 | Container could be running with outdated image | [] | [] | e-corp-demo/goof-kubernetes(master):goof-deployment.yaml | | Not Auto Fixable | 2023-03-07 23:04:06.635 | Snyk IaC |
| Low | 250 | Container is running without memory limit | [] | [] | e-corp-demo/goof-kubernetes(master):goof-deployment.yaml | | Not Auto Fixable | 2023-03-07 23:04:06.635 | Snyk IaC |
| Low | 250 | Container is running with writable root filesystem | [] | [] | e-corp-demo/goof-kubernetes(master):goof-mongo-deployment.yaml | | Not Auto Fixable | 2023-03-07 23:04:06.675 | Snyk IaC |
| Low | 250 | Container's UID could clash with host's UID | [] | [] | e-corp-demo/goof-kubernetes(master):goof-mongo-deployment.yaml | | Not Auto Fixable | 2023-03-15 14:01:21.899 | Snyk IaC |
| Low | 250 | Container has no CPU limit | [] | [] | e-corp-demo/goof-kubernetes(master):goof-mongo-deployment.yaml | | Not Auto Fixable | 2023-03-07 23:04:06.675 | Snyk IaC |
| Low | 221 | CVE-2023-1972 | ["CVE-2023-1972"] | [] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-04-15 05:30:58.746 | Snyk Container |
| Low | 221 | Arbitrary Code Injection | ["CVE-2023-29007"] | ["CWE-74"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-04-26 06:06:25.919 | Snyk Container |
| Low | 221 | Arbitrary Code Injection | ["CVE-2023-29007"] | ["CWE-74"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-04-27 01:13:15.939 | Snyk Container |
| Low | 221 | Use of Externally-Controlled Format String | ["CVE-2023-25815"] | ["CWE-134", "CWE-22"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-04-27 01:13:15.939 | Snyk Container |
| Low | 221 | Arbitrary Code Injection | ["CVE-2023-29383"] | ["CWE-74"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-04-15 19:19:14.675 | Snyk Container |
| Low | 221 | Arbitrary Code Injection | ["CVE-2023-29383"] | ["CWE-74"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-04-15 19:53:05.953 | Snyk Container |
| Low | 221 | Use of Externally-Controlled Format String | ["CVE-2023-25815"] | ["CWE-134", "CWE-22"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-04-26 06:06:25.919 | Snyk Container |
| Low | 221 | Out-of-bounds Read | ["CVE-2023-1916"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-04-08 21:08:54.275 | Snyk Container |
| Low | 221 | Directory Traversal | ["CVE-2023-25652"] | ["CWE-22"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-04-27 01:13:15.939 | Snyk Container |
| Low | 221 | Directory Traversal | ["CVE-2023-25652"] | ["CWE-22"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-04-26 06:06:25.919 | Snyk Container |
| Low | 221 | Improper Input Validation | ["CVE-2023-27043"] | ["CWE-20"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-04-21 04:59:08.612 | Snyk Container |
| Low | 221 | CVE-2023-30775 | ["CVE-2023-30775"] | [] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-04-19 19:39:07.214 | Snyk Container |
| Low | 221 | Out-of-bounds Write | ["CVE-2023-1579"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-04-08 21:08:54.274 | Snyk Container |
| Low | 221 | CVE-2023-30774 | ["CVE-2023-30774"] | [] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-04-19 19:39:07.214 | Snyk Container |
| Medium | 215 | Improper Input Validation | ["CVE-2021-22060"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| Medium | 215 | Improper Output Neutralization for Logs | ["CVE-2021-22096"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/todolist-web-common/pom.xml | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:30.835 | Snyk Open Source |
| Low | 150 | Improper Authentication | ["CVE-2023-27538"] | ["CWE-287"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-21 18:40:28.583 | Snyk Container |
| Low | 150 | Resource Exhaustion | ["CVE-2021-3733"] | ["CWE-400"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|--------------------|-----------------------|--|------------------|------------------|-------------------------|----------------|
| Low | 150 | Link Following | ["CVE-2013-4392"] | ["CWE-59"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2018-7470"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Divide By Zero | ["CVE-2014-8130"] | ["CWE-369"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2018-18701"] | ["CWE-835"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2021-4209"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2018-5357"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Origin Validation Error | ["CVE-2017-6519"] | ["CWE-346"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2020-35522"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-12665"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | CVE-2018-3136 | ["CVE-2018-3136"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2023-27102"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-16 18:52:47.113 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-12669"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-9752"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2018-9135"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | CVE-2018-12698 | ["CVE-2018-12698"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Use After Free | ["CVE-2021-36086"] | ["CWE-416"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Information Exposure | ["CVE-2018-16869"] | ["CWE-203"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2017-13685"] | ["CWE-20"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2017-9814"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Allocation of Resources Without Limits or Throttling | ["CVE-2023-25193"] | ["CWE-770"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Memory Leak | ["CVE-2021-45346"] | ["CWE-401"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Divide By Zero | ["CVE-2021-20245"] | ["CWE-369"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2019-12972"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-9744"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Information Exposure | ["CVE-2019-19126"] | ["CWE-200"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Resource Management Errors | ["CVE-2010-4756"] | ["CWE-399"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2018-20673"] | ["CWE-787","CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Arbitrary Code Injection | ["CVE-2017-17522"] | ["CWE-74"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|--------------------|------------------------|--|------------------|------------------|-------------------------|----------------|
| Low | 150 | Out-of-bounds Write | ["CVE-2017-12459"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2016-9085"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Use After Free | ["CVE-2020-16592"] | ["CWE-416"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.449 | Snyk Container |
| Low | 150 | Cryptographic Issues | ["CVE-2015-3276"] | ["CWE-310"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2016-9117"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Uncontrolled Recursion | ["CVE-2019-9904"] | ["CWE-674"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2023-27103"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-16 18:52:47.113 | Snyk Container |
| Low | 150 | Divide By Zero | ["CVE-2018-20845"] | ["CWE-369"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Uncontrolled Recursion | ["CVE-2018-20796"] | ["CWE-674"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Link Following | ["CVE-2011-4116"] | ["CWE-59"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Uncontrolled Recursion | ["CVE-2021-3530"] | ["CWE-674"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-9748"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | CVE-2020-14577 | ["CVE-2020-14577"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2018-18483"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Resource Exhaustion | ["CVE-2018-15607"] | ["CWE-400"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2018-14550"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-15218"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | CVE-2019-2983 | ["CVE-2019-2983"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Allocation of Resources Without Limits or Throttling | ["CVE-2017-13716"] | ["CWE-770"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2016-2781"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-12641"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2019-20838"] | ["CWE-125"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2018-6951"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | CVE-2016-20012 | ["CVE-2016-20012"] | [] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2018-20671"] | ["CWE-787", "CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Arbitrary Command Injection | ["CVE-2015-20107"] | ["CWE-77"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2021-39537"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-18254"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|----------------------|-------------|--|------------------|------------------|-------------------------|----------------|
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2020-35457"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2019-17543"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Use of Insufficiently Random Values | ["CVE-2019-1010025"] | ["CWE-330"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Resource Exhaustion | ["CVE-2022-45061"] | ["CWE-400"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-6502"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Cryptographic Issues | ["CVE-2010-0928"] | ["CWE-310"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Open Redirect | ["CVE-2021-31879"] | ["CWE-601"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2018-7999"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Improper Initialization | ["CVE-2017-14159"] | ["CWE-665"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2021-3575"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-16232"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Divide By Zero | ["CVE-2021-20311"] | ["CWE-369"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-12654"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Cross-site Request Forgery (CSRF) | ["CVE-2018-1000858"] | ["CWE-352"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | CVE-2018-2952 | ["CVE-2018-2952"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Link Following | ["CVE-2013-4392"] | ["CWE-59"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2017-9117"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2016-9800"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Divide By Zero | ["CVE-2016-10506"] | ["CWE-369"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Information Exposure | ["CVE-2018-15919"] | ["CWE-200"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2019-17595"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Incorrect Type Conversion or Cast | ["CVE-2020-10735"] | ["CWE-704"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2017-7475"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Use of Insufficiently Random Values | ["CVE-2019-1010025"] | ["CWE-330"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2017-9117"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Memory Leak | ["CVE-2019-6129"] | ["CWE-401"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Use After Free | ["CVE-2021-36086"] | ["CWE-416"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | CVE-2020-2654 | ["CVE-2020-2654"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|--------------------|---------------------------------|--|------------------|------------------|-------------------------|----------------|
| Low | 150 | Allocation of Resources Without Limits or Throttling | ["CVE-2018-12934"] | ["CWE-770"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2018-6951"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | CVE-2020-14578 | ["CVE-2020-14578"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Cryptographic Issues | ["CVE-2015-3276"] | ["CWE-310"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Cryptographic Issues | ["CVE-2012-0039"] | ["CWE-310"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-12799"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2022-27404"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | Link Following | ["CVE-2021-20197"] | ["CWE-59"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2019-9169"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Use After Free | ["CVE-2018-15857"] | ["CWE-416"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Memory Leak | ["CVE-2021-45346"] | ["CWE-401"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | CVE-2005-2541 | ["CVE-2005-2541"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Reachable Assertion | ["CVE-2018-10963"] | ["CWE-617"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2017-12453"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-11695"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2016-9116"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Improper Verification of Cryptographic Signature | ["CVE-2011-3374"] | ["CWE-347"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2019-16709"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2018-18607"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-9753"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2016-9581"] | ["CWE-119","CWE-122","CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2020-35448"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | XML External Entity (XXE) Injection | ["CVE-2013-0340"] | ["CWE-611"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2022-29458"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Low | 150 | Use After Free | ["CVE-2020-11656"] | ["CWE-416"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Buffer Overflow | ["CVE-2019-8842"] | ["CWE-120"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | Improper Certificate Validation | ["CVE-2023-0466"] | ["CWE-295"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-29 17:34:07.507 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|--------------------|----------------------------------|--|------------------|------------------|-------------------------|----------------|
| Low | 150 | CVE-2008-1688 | ["CVE-2008-1688"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | CVE-2023-22606 | ["CVE-2023-22606"] | [] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Resource Exhaustion | ["CVE-2018-15607"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2018-18605"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Improper Resource Shutdown or Release | ["CVE-2019-6488"] | ["CWE-404"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2021-45942"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2018-16888"] | ["CWE-20", "CWE-732", "CWE-732"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2016-10739"] | ["CWE-20"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Information Exposure | ["CVE-2022-0563"] | ["CWE-209"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-17934"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2017-15023"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2018-5709"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2016-10228"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | Cryptographic Issues | ["CVE-2012-0039"] | ["CWE-310"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | Memory Leak | ["CVE-2019-6128"] | ["CWE-401"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2018-20846"] | ["CWE-20"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Access Restriction Bypass | ["CVE-2007-5686"] | ["CWE-264"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Allocation of Resources Without Limits or Throttling | ["CVE-2018-13033"] | ["CWE-770"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Directory Traversal | ["CVE-2010-4651"] | ["CWE-22"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Use After Free | ["CVE-2017-17973"] | ["CWE-416"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2019-16708"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | CVE-2022-4415 | ["CVE-2022-4415"] | [] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | CVE-2019-2988 | ["CVE-2019-2988"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Improper Certificate Validation | ["CVE-2020-15719"] | ["CWE-295"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Insufficient Verification of Data Authenticity | ["CVE-2021-40491"] | ["CWE-345"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2018-15856"] | ["CWE-835"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2018-5358"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|---------------------|-------------|--|------------------|------------------|-------------------------|----------------|
| Low | 150 | Resource Exhaustion | ["CVE-2021-3733"] | ["CWE-400"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Uncontrolled Recursion | ["CVE-2019-9192"] | ["CWE-674"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2018-10805"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-9937"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.455 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2017-15022"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-12667"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Use of Uninitialized Resource | ["CVE-2020-35494"] | ["CWE-908"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.449 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-9745"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Improper Verification of Cryptographic Signature | ["CVE-2011-3374"] | ["CWE-347"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.449 | Snyk Container |
| Low | 150 | Improper Verification of Cryptographic Signature | ["CVE-2011-3374"] | ["CWE-347"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2011-3389"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Link Following | ["CVE-2021-21300"] | ["CWE-59"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2018-7643"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2021-3549"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2022-29458"] | ["CWE-125"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2018-7570"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2018-16750"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Uncontrolled Recursion | ["CVE-2017-11164"] | ["CWE-674"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-9747"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2018-18443"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2017-14933"] | ["CWE-835"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2017-100082"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Buffer Overflow | ["CVE-2023-0996"] | ["CWE-120"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2018-18064"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | Memory Leak | ["CVE-2019-10649"] | ["CWE-401"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Buffer Overflow | ["CVE-2021-4214"] | ["CWE-120"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Memory Leak | ["CVE-2019-13301"] | ["CWE-401"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2022-38533"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|--------------------|-------------|--|------------------|------------------|-------------------------|----------------|
| Low | 150 | Uncontrolled Recursion | ["CVE-2018-18484"] | ["CWE-674"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Numeric Errors | ["CVE-2007-3996"] | ["CWE-189"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Improper Certificate Validation | ["CVE-2023-0464"] | ["CWE-295"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-23 16:53:51.630 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2017-15021"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Resource Exhaustion | ["CVE-2022-4899"] | ["CWE-400"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-04-05 02:05:46.750 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-9749"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Improper Data Handling | ["CVE-2015-8985"] | ["CWE-19"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | XML External Entity (XXE) Injection | ["CVE-2013-0340"] | ["CWE-611"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | CVE-2019-7309 | ["CVE-2019-7309"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-18027"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2022-3715"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Use After Free | ["CVE-2021-36085"] | ["CWE-416"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Divide By Zero | ["CVE-2021-3941"] | ["CWE-369"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-7246"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-17883"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Authentication Bypass | ["CVE-2020-13529"] | ["CWE-290"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-12644"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2017-6311"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2021-20294"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.449 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2022-32545"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Exposure of Resource to Wrong Sphere | ["CVE-2022-24975"] | ["CWE-668"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Improper Validation of Integrity Check Value | ["CVE-2021-22922"] | ["CWE-354"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2018-7648"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2022-0204"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-12664"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2020-1751"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-11534"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-11531"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|--------------------|-------------|--|------------------|------------------|-------------------------|----------------|
| Low | 150 | Out-of-bounds Read | ["CVE-2017-9814"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-13058"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Arbitrary Code Injection | ["CVE-2022-0391"] | ["CWE-74"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Cryptographic Issues | ["CVE-2007-6755"] | ["CWE-310"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2017-15016"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2017-12458"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2019-6462"] | ["CWE-835"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | Incorrect Permission Assignment for Critical Resource | ["CVE-2018-7169"] | ["CWE-732"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-18251"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Incorrect Permission Assignment for Critical Resource | ["CVE-2019-19882"] | ["CWE-732"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Directory Traversal | ["CVE-2023-27534"] | ["CWE-22"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-21 16:47:40.962 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2011-3389"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2011-3389"] | ["CWE-20"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Use of Incorrectly-Resolved Name or Reference | ["CVE-2019-1351"] | ["CWE-706"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2017-9038"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-17740"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-14138"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Double Free | ["CVE-2021-27645"] | ["CWE-415"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2017-9954"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Information Exposure | ["CVE-2020-14145"] | ["CWE-200"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2017-12652"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-11755"] | ["CWE-772"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Access Restriction Bypass | ["CVE-2008-3234"] | ["CWE-264"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Memory Leak | ["CVE-2019-3815"] | ["CWE-401"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2017-9043"] | ["CWE-20"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Memory Leak | ["CVE-2020-27753"] | ["CWE-401"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Unchecked Return Value | ["CVE-2021-4189"] | ["CWE-252"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2021-35942"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|--------------------|-------------------|--|------------------|------------------|-------------------------|----------------|
| Low | 150 | Improper Input Validation | ["CVE-2016-2781"] | ["CWE-20"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Resource Exhaustion | ["CVE-2022-45061"] | ["CWE-400"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2020-35496"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.449 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-14930"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Access Restriction Bypass | ["CVE-2008-3234"] | ["CWE-264"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Open Redirect | ["CVE-2021-31879"] | ["CWE-601"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.457 | Snyk Container |
| Low | 150 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2019-6462"] | ["CWE-835"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Memory Leak | ["CVE-2019-12976"] | ["CWE-401"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Access Restriction Bypass | ["CVE-2008-3234"] | ["CWE-264"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-9756"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2022-1115"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | CVE-2020-2756 | ["CVE-2020-2756"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Memory Leak | ["CVE-2019-6129"] | ["CWE-401"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Integer Underflow | ["CVE-2021-26945"] | ["CWE-191","CWE-" | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | CVE-2020-14779 | ["CVE-2020-14779"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Low | 150 | Information Exposure | ["CVE-2021-20313"] | ["CWE-200"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2021-20284"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.449 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2018-10535"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Improper Certificate Validation | ["CVE-2023-0465"] | ["CWE-295"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-29 17:34:07.507 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2016-9917"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2022-27405"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2018-10373"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2018-13153"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | CVE-2008-1687 | ["CVE-2008-1687"] | [] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Reachable Assertion | ["CVE-2019-6461"] | ["CWE-617"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Uncontrolled Search Path Element | ["CVE-2022-24765"] | ["CWE-427"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | CVE-2019-2973 | ["CVE-2019-2973"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Improper Authentication | ["CVE-2007-2243"] | ["CWE-287"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|--------------------|------------------------|--|------------------|------------------|-------------------------|----------------|
| Low | 150 | Out-of-Bounds | ["CVE-2017-16826"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2016-8678"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-15217"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Arbitrary Code Injection | ["CVE-2022-0391"] | ["CWE-74"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | CVE-2005-0406 | ["CVE-2005-0406"] | [] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2014-8166"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | CVE-2018-2579 | ["CVE-2018-2579"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2020-35507"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.449 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2021-3487"] | ["CWE-20", "CWE-400"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.449 | Snyk Container |
| Low | 150 | Resource Management Errors | ["CVE-2007-3477"] | ["CWE-399"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-11754"] | ["CWE-772"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Time-of-check Time-of-use (TOCTOU) | ["CVE-2013-4235"] | ["CWE-367"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Time-of-check Time-of-use (TOCTOU) | ["CVE-2013-4235"] | ["CWE-367"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Link Following | ["CVE-2011-4116"] | ["CWE-59"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Double Free | ["CVE-2020-16590"] | ["CWE-415"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.449 | Snyk Container |
| Low | 150 | Resource Exhaustion | ["CVE-2018-17985"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2020-27752"] | ["CWE-787", "CWE-415"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2020-36332"] | ["CWE-20", "CWE-400"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2016-10505"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Information Exposure | ["CVE-2021-33560"] | ["CWE-203"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | CVE-2020-14782 | ["CVE-2020-14782"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Low | 150 | Improper Verification of Cryptographic Signature | ["CVE-2011-3374"] | ["CWE-347"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Double Free | ["CVE-2017-11462"] | ["CWE-415"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Divide By Zero | ["CVE-2014-8130"] | ["CWE-369"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | CVE-2023-22603 | ["CVE-2023-22603"] | [] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2022-27404"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Exposure of Resource to Wrong Sphere | ["CVE-2021-39212"] | ["CWE-668"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2022-31782"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|----------------------|-------------|--|------------------|------------------|-------------------------|----------------|
| Low | 150 | CVE-2005-2541 | ["CVE-2005-2541"] | [] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | CVE-2005-2541 | ["CVE-2005-2541"] | [] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2018-15863"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Low | 150 | CVE-2019-1010023 | ["CVE-2019-1010023"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Integer Underflow | ["CVE-2020-6096"] | ["CWE-191"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Numeric Errors | ["CVE-2007-3476"] | ["CWE-189"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Allocation of Resources Without Limits or Throttling | ["CVE-2019-6988"] | ["CWE-770"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-7245"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | LDAP Injection | ["CVE-2018-5730"] | ["CWE-90"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.455 | Snyk Container |
| Low | 150 | Link Following | ["CVE-2013-4392"] | ["CWE-59"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Cryptographic Issues | ["CVE-2010-0928"] | ["CWE-310"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2020-36130"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Allocation of Resources Without Limits or Throttling | ["CVE-2017-18028"] | ["CWE-770"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | CVE-2019-1010023 | ["CVE-2019-1010023"] | [] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2021-20304"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2018-16375"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Improper Authentication | ["CVE-2021-36368"] | ["CWE-287"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Uncontrolled Recursion | ["CVE-2018-9996"] | ["CWE-674"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2018-6543"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Improper Validation of Array Index | ["CVE-2022-35737"] | ["CWE-129"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Improper Validation of Array Index | ["CVE-2022-35737"] | ["CWE-129"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Security Features | ["CVE-2016-1585"] | ["CWE-254"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | Improper Verification of Cryptographic Signature | ["CVE-2020-16156"] | ["CWE-347"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Off-by-one Error | ["CVE-2021-3999"] | ["CWE-193"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Numeric Errors | ["CVE-2007-3996"] | ["CWE-189"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Insufficiently Protected Credentials | ["CVE-2021-22923"] | ["CWE-522"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | CVE-2021-3601 | ["CVE-2021-3601"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2018-1000021"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|----------------------|------------------|--|------------------|------------------|-------------------------|----------------|
| Low | 150 | Improper Input Validation | ["CVE-2018-8945"] | ["CWE-20"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2021-3549"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.449 | Snyk Container |
| Low | 150 | CVE-2019-1010023 | ["CVE-2019-1010023"] | [] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2020-35522"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | OS Command Injection | ["CVE-2020-15778"] | ["CWE-78"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | CVE-2019-2987 | ["CVE-2019-2987"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-16827"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Use After Free | ["CVE-2022-1114"] | ["CWE-416"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Resource Exhaustion | ["CVE-2021-3737"] | ["CWE-400","CWE- | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2017-9955"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-9937"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-15996"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Information Exposure | ["CVE-2022-0563"] | ["CWE-209"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2016-9113"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Improper Privilege Management | ["CVE-2021-41617"] | ["CWE-269"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2016-9117"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Improper Authentication | ["CVE-2023-27535"] | ["CWE-287"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-21 16:47:40.962 | Snyk Container |
| Low | 150 | Divide By Zero | ["CVE-2019-15133"] | ["CWE-369"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | Use After Free | ["CVE-2021-36084"] | ["CWE-416"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Access Restriction Bypass | ["CVE-2016-2779"] | ["CWE-264"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2017-12450"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-18008"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-13062"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2016-9804"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Memory Leak | ["CVE-2019-7396"] | ["CWE-401"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2016-9803"] | ["CWE-119","CWE- | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2018-14437"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2016-10505"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|----------------------|-----------------------|--|------------------|------------------|-------------------------|----------------|
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-11532"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Authentication Bypass | ["CVE-2020-13529"] | ["CWE-290"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-12672"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2018-11489"] | ["CWE-787","CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | CVE-2023-22609 | ["CVE-2023-22609"] | [] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2018-14550"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Double Free | ["CVE-2021-40145"] | ["CWE-415"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2021-38115"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2017-12652"] | ["CWE-20"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Buffer Overflow | ["CVE-2022-23218"] | ["CWE-120"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2017-15232"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2017-15232"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | OS Command Injection | ["CVE-2020-15778"] | ["CWE-78"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2023-0634"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | CVE-2019-2422 | ["CVE-2019-2422"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-14533"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | CVE-2019-2981 | ["CVE-2019-2981"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2022-31782"] | ["CWE-787"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2018-1000876"] | ["CWE-787","CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2017-16830"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2016-9114"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2021-4209"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Privilege Chaining | ["CVE-2019-3844"] | ["CWE-268"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2018-17983"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2017-12449"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Resource Exhaustion | ["CVE-2017-14988"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Key Management Errors | ["CVE-2018-9234"] | ["CWE-320"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Key Management Errors | ["CVE-2018-9234"] | ["CWE-320"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|--------------------|------------------------|--|------------------|------------------|-------------------------|----------------|
| Low | 150 | Out-of-bounds Read | ["CVE-2017-9041"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | CVE-2008-1688 | ["CVE-2008-1688"] | [] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2017-16832"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2017-12451"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2019-14444"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2017-13710"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2018-18606"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Information Exposure | ["CVE-2020-1968"] | ["CWE-203"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Information Exposure | ["CVE-2020-1968"] | ["CWE-203"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2019-16713"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2018-20712"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2021-36087"] | ["CWE-125"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-17884"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2019-8905"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2017-8871"] | ["CWE-835"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2020-23922"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2017-14333"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Use of Insufficiently Random Values | ["CVE-2015-9019"] | ["CWE-330"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Resource Exhaustion | ["CVE-2017-14342"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | CVE-2019-2992 | ["CVE-2019-2992"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2018-5247"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Memory Leak | ["CVE-2019-7175"] | ["CWE-401"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2021-20193"] | ["CWE-125", "CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2021-4217"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-7245"] | ["CWE-119"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | CVE-2016-20012 | ["CVE-2016-20012"] | [] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Improper Validation of Integrity Check Value | ["CVE-2021-22922"] | ["CWE-354"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-16232"] | ["CWE-772"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|--------------------|-----------------------|--|------------------|------------------|-------------------------|----------------|
| Low | 150 | CVE-2018-2790 | ["CVE-2018-2790"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2019-7149"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2022-33068"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2022-33068"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2020-16591"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.449 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2018-10804"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-16231"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2021-20193"] | ["CWE-125","CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Directory Traversal | ["CVE-2023-27534"] | ["CWE-22"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-21 18:40:28.583 | Snyk Container |
| Low | 150 | Improper Validation of Integrity Check Value | ["CVE-2021-22922"] | ["CWE-354"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Improper Certificate Validation | ["CVE-2023-0465"] | ["CWE-295"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-29 22:23:50.983 | Snyk Container |
| Low | 150 | Allocation of Resources Without Limits or Throttling | ["CVE-2019-6988"] | ["CWE-770"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2022-27405"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2022-47015"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Information Exposure | ["CVE-2007-2379"] | ["CWE-200"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.455 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2018-11655"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-11751"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2017-7475"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2018-14435"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | PRNG Seed Error | ["CVE-2018-12384"] | ["CWE-335"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2020-14155"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Use After Free | ["CVE-2020-11656"] | ["CWE-416"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2018-17965"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2020-17541"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2020-17541"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Allocation of Resources Without Limits or Throttling | ["CVE-2019-9073"] | ["CWE-770"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.449 | Snyk Container |
| Low | 150 | Improper Resource Shutdown or Release | ["CVE-2019-6488"] | ["CWE-404"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2019-9169"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|----------------------|---------------------------------|--|------------------|------------------|-------------------------|----------------|
| Low | 150 | Improper Input Validation | ["CVE-2020-13776"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Information Exposure | ["CVE-2018-16869"] | ["CWE-203"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-13060"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2021-45078"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-17886"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-17126"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2017-16829"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Improper Initialization | ["CVE-2017-14159"] | ["CWE-665"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2017-17479"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2019-8457"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2019-8457"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | CVE-2019-1010023 | ["CVE-2019-1010023"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2016-9581"] | ["CWE-119","CWE-122","CWE-401"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Memory Leak | ["CVE-2019-13309"] | ["CWE-401"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2018-18661"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Improper Initialization | ["CVE-2022-1122"] | ["CWE-665","CWE-416"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Use After Free | ["CVE-2017-17973"] | ["CWE-416"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | CVE-2022-4415 | ["CVE-2022-4415"] | [] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Improper Verification of Cryptographic Signature | ["CVE-2020-16156"] | ["CWE-347"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2023-24329"] | ["CWE-20"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2023-24329"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2018-12697"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2018-100021"] | ["CWE-20"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-11754"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Uncontrolled Recursion | ["CVE-2019-9192"] | ["CWE-674"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Improper Verification of Cryptographic Signature | ["CVE-2020-16156"] | ["CWE-347"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-9937"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|----------------------|-----------------------|--|------------------|------------------|-------------------------|----------------|
| Low | 150 | Out-of-bounds Write | ["CVE-2018-19931"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2022-32545"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | CVE-2023-22604 | ["CVE-2023-22604"] | [] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Uncontrolled Recursion | ["CVE-2019-17450"] | ["CWE-674"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Divide By Zero | ["CVE-2021-20309"] | ["CWE-369"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Race Condition | ["CVE-2019-13627"] | ["CWE-362"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2018-5710"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.455 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2017-17880"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2011-3389"] | ["CWE-20"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-12663"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2019-1010022"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2021-45078"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.449 | Snyk Container |
| Low | 150 | CVE-2020-2754 | ["CVE-2020-2754"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Unchecked Return Value | ["CVE-2021-4189"] | ["CWE-252"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2019-20838"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2018-15859"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Low | 150 | Uncontrolled Recursion | ["CVE-2021-46195"] | ["CWE-674"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.449 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2017-14128"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2022-1056"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Integer Underflow | ["CVE-2021-26945"] | ["CWE-191","CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2022-29458"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2018-19932"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Allocation of Resources Without Limits or Throttling | ["CVE-2017-14938"] | ["CWE-770"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2019-25013"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | CVE-2018-1000654 | ["CVE-2018-1000654"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2018-17794"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Uncontrolled Recursion | ["CVE-2021-3997"] | ["CWE-674"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2018-20651"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|----------------------|-----------------------|--|------------------|------------------|-------------------------|----------------|
| Low | 150 | Information Exposure | ["CVE-2022-0563"] | ["CWE-209"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.457 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2020-25664"] | ["CWE-787","CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2017-13757"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-15033"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Incorrect Default Permissions | ["CVE-2017-15131"] | ["CWE-276","CWE-327"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Use of a Broken or Risky Cryptographic Algorithm | ["CVE-2018-6829"] | ["CWE-327"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Use After Free | ["CVE-2021-36085"] | ["CWE-416"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Use After Free | ["CVE-2021-36085"] | ["CWE-416"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Use After Free | ["CVE-2021-36085"] | ["CWE-416"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2018-18016"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | CVE-2020-2757 | ["CVE-2020-2757"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-12666"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Improper Authentication | ["CVE-2023-27536"] | ["CWE-287"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-21 18:40:28.583 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2020-36131"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Information Exposure | ["CVE-2019-1010024"] | ["CWE-200"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Information Exposure | ["CVE-2019-1010024"] | ["CWE-200"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Reachable Assertion | ["CVE-2019-6461"] | ["CWE-617"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2022-3715"] | ["CWE-787"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Use of Insufficiently Random Values | ["CVE-2019-1010025"] | ["CWE-330"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2018-14434"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-15088"] | ["CWE-119","CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.455 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2018-16376"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2018-18309"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Uncontrolled Recursion | ["CVE-2019-9071"] | ["CWE-674"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.449 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2018-15855"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Low | 150 | Unchecked Return Value | ["CVE-2021-4189"] | ["CWE-252"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Allocation of Resources Without Limits or Throttling | ["CVE-2017-12132"] | ["CWE-770"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Use of Insufficiently Random Values | ["CVE-2019-1010025"] | ["CWE-330"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|----------------------|-----------------------|--|------------------|------------------|-------------------------|----------------|
| Low | 150 | NULL Pointer Dereference | ["CVE-2023-0634"] | ["CWE-476"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2017-12676"] | ["CWE-20","CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2019-20838"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-12982"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Information Exposure | ["CVE-2007-2768"] | ["CWE-200"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2022-31782"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2017-12457"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2019-1010180"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Use After Free | ["CVE-2017-17973"] | ["CWE-416"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2019-6462"] | ["CWE-835"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-11536"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | CVE-2022-39176 | ["CVE-2022-39176"] | [] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2021-4217"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Improper Initialization | ["CVE-2017-14159"] | ["CWE-665"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | CVE-2019-2842 | ["CVE-2019-2842"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Incorrect Privilege Assignment | ["CVE-2019-3843"] | ["CWE-266"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | OS Command Injection | ["CVE-2020-15778"] | ["CWE-78"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2018-16866"] | ["CWE-125","CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Resource Management Errors | ["CVE-2008-3134"] | ["CWE-399"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Link Following | ["CVE-2021-20197"] | ["CWE-59"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.449 | Snyk Container |
| Low | 150 | Buffer Overflow | ["CVE-2022-23218"] | ["CWE-120"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2017-14529"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Allocation of Resources Without Limits or Throttling | ["CVE-2017-9039"] | ["CWE-770"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2018-5709"] | ["CWE-190"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | CVE-2017-10345 | ["CVE-2017-10345"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-12418"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2016-10228"] | ["CWE-20"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | LDAP Injection | ["CVE-2018-5730"] | ["CWE-90"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|----------------------|-----------------------|--|------------------|------------------|-------------------------|----------------|
| Low | 150 | Cryptographic Issues | ["CVE-2012-0039"] | ["CWE-310"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-7245"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Memory Leak | ["CVE-2019-6128"] | ["CWE-401"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2017-17122"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2022-32546"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2019-1010204"] | ["CWE-20","CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2019-1354"] | ["CWE-20"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Buffer Overflow | ["CVE-2021-4214"] | ["CWE-120"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Cryptographic Issues | ["CVE-2015-3276"] | ["CWE-310"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Link Following | ["CVE-2011-4116"] | ["CWE-59"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Resource Exhaustion | ["CVE-2021-41229"] | ["CWE-400"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2016-9797"] | ["CWE-119","CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2017-17125"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-18022"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2018-20712"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Race Condition | ["CVE-2017-18018"] | ["CWE-362"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2018-7208"] | ["CWE-20"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2018-20673"] | ["CWE-787","CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2018-15864"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2020-35457"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Open Redirect | ["CVE-2021-31879"] | ["CWE-601"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2019-1350"] | ["CWE-20"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | CVE-2021-35603 | ["CVE-2021-35603"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Low | 150 | Improper Authentication | ["CVE-2007-2243"] | ["CWE-287"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2017-9040"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-17680"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Memory Leak | ["CVE-2019-12975"] | ["CWE-401"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Uncontrolled Recursion | ["CVE-2019-9192"] | ["CWE-674"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|--------------------|-------------|--|------------------|------------------|-------------------------|----------------|
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2018-16640"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2017-9117"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Resource Exhaustion | ["CVE-2017-14137"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Incorrect Type Conversion or Cast | ["CVE-2020-10735"] | ["CWE-704"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Incorrect Type Conversion or Cast | ["CVE-2022-32547"] | ["CWE-704"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Resource Exhaustion | ["CVE-2022-1210"] | ["CWE-400"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Memory Leak | ["CVE-2019-13310"] | ["CWE-401"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Cross-site Scripting (XSS) | ["CVE-2016-3709"] | ["CWE-79"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Uncontrolled Recursion | ["CVE-2018-9996"] | ["CWE-674"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2016-10739"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2018-14436"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2019-8457"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Exposure of Resource to Wrong Sphere | ["CVE-2021-39212"] | ["CWE-668"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | CVE-2021-2341 | ["CVE-2021-2341"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-17740"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-17740"] | ["CWE-119"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Buffer Overflow | ["CVE-2022-28463"] | ["CWE-120"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2020-1751"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2020-35521"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-7245"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2009-3546"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2018-18544"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | CVE-2022-41862 | ["CVE-2022-41862"] | [] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | CVE-2020-14796 | ["CVE-2020-14796"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Low | 150 | Use After Free | ["CVE-2016-9798"] | ["CWE-416"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2023-1289"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-15 12:41:03.844 | Snyk Container |
| Low | 150 | Memory Leak | ["CVE-2019-13311"] | ["CWE-401"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Use After Free | ["CVE-2021-36084"] | ["CWE-416"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|----------------------|-----------------------|--|------------------|------------------|-------------------------|----------------|
| Low | 150 | Use After Free | ["CVE-2021-36084"] | ["CWE-416"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2009-3546"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Buffer Overflow | ["CVE-2021-4214"] | ["CWE-120"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2018-7569"] | ["CWE-190","CWE-120"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2018-20846"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-16231"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2018-15858"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Low | 150 | Open Redirect | ["CVE-2021-31879"] | ["CWE-601"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-11752"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2020-13776"] | ["CWE-20"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Use After Free | ["CVE-2021-36086"] | ["CWE-416"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-12673"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Resource Exhaustion | ["CVE-2021-3737"] | ["CWE-400","CWE-120"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2021-3487"] | ["CWE-20","CWE-400"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Use After Free | ["CVE-2021-36086"] | ["CWE-416"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Origin Validation Error | ["CVE-2017-6519"] | ["CWE-346"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.449 | Snyk Container |
| Low | 150 | Link Following | ["CVE-2008-4108"] | ["CWE-59"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2022-33068"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Information Exposure | ["CVE-2021-33560"] | ["CWE-203"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Information Exposure | ["CVE-2021-33560"] | ["CWE-203"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Buffer Overflow | ["CVE-2020-36133"] | ["CWE-120"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Integer Underflow | ["CVE-2020-6096"] | ["CWE-191"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-15032"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2021-20284"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2020-35448"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.449 | Snyk Container |
| Low | 150 | Memory Leak | ["CVE-2019-6129"] | ["CWE-401"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2019-1010204"] | ["CWE-20","CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Improper Certificate Validation | ["CVE-2020-15719"] | ["CWE-295"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|----------------------|-------------|--|------------------|------------------|-------------------------|----------------|
| Low | 150 | CVE-2022-42919 | ["CVE-2022-42919"] | [] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2017-12456"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | CVE-2020-27619 | ["CVE-2020-27619"] | [] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | CVE-2021-3601 | ["CVE-2021-3601"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Access Restriction Bypass | ["CVE-2007-5686"] | ["CWE-264"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2018-16403"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2018-16403"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2021-37600"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.457 | Snyk Container |
| Low | 150 | Information Exposure | ["CVE-2019-19126"] | ["CWE-200"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2019-9923"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | CVE-2020-14781 | ["CVE-2020-14781"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Low | 150 | Access Restriction Bypass | ["CVE-2007-5686"] | ["CWE-264"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Race Condition | ["CVE-2019-13627"] | ["CWE-362"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2018-5710"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Uncontrolled Recursion | ["CVE-2021-3530"] | ["CWE-674"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.449 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-17881"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-14684"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2019-1010022"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2020-16599"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.449 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2018-5246"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | CVE-2020-2755 | ["CVE-2020-2755"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Resource Exhaustion | ["CVE-2019-9674"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Double Free | ["CVE-2017-11462"] | ["CWE-415"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.455 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2017-14745"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | CVE-2016-20012 | ["CVE-2016-20012"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2021-29338"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Use of a Broken or Risky Cryptographic Algorithm | ["CVE-2019-14855"] | ["CWE-327"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2022-1056"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|--------------------|-----------------------|--|------------------|------------------|-------------------------|----------------|
| Low | 150 | NULL Pointer Dereference | ["CVE-2016-9114"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-9743"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Link Following | ["CVE-2011-4116"] | ["CWE-59"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Uncontrolled Recursion | ["CVE-2017-11164"] | ["CWE-674"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-11724"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Uncontrolled Recursion | ["CVE-2021-3997"] | ["CWE-674"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2017-11335"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Improper Privilege Management | ["CVE-2021-41617"] | ["CWE-269"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2018-18064"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2018-15861"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-12564"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Double Free | ["CVE-2018-6952"] | ["CWE-415"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2020-27618"] | ["CWE-835"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2019-14250"] | ["CWE-787","CWE-611"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | XML External Entity (XXE) Injection | ["CVE-2013-0340"] | ["CWE-611"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | CVE-2019-7309 | ["CVE-2019-7309"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Uncontrolled Recursion | ["CVE-2017-11164"] | ["CWE-674"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Cryptographic Issues | ["CVE-2007-6755"] | ["CWE-310"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-7275"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | CVE-2020-2773 | ["CVE-2020-2773"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2018-17359"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Improper Privilege Management | ["CVE-2021-41617"] | ["CWE-269"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Incorrect Permission Assignment for Critical Resource | ["CVE-2019-19882"] | ["CWE-732"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2022-32546"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Use of a Broken or Risky Cryptographic Algorithm | ["CVE-2018-6829"] | ["CWE-327"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | CVE-2022-21248 | ["CVE-2022-21248"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Low | 150 | Time-of-check Time-of-use (TOCTOU) | ["CVE-2013-4235"] | ["CWE-367"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Time-of-check Time-of-use (TOCTOU) | ["CVE-2013-4235"] | ["CWE-367"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|---|--------------------|------------------------|--|------------------|------------------|-------------------------|----------------|
| Low | 150 | Out-of-bounds Read | ["CVE-2017-9044"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.449 | Snyk Container |
| Low | 150 | CVE-2022-21443 | ["CVE-2022-21443"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2017-12455"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Access Restriction Bypass | ["CVE-2016-2779"] | ["CWE-264"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.457 | Snyk Container |
| Low | 150 | Resource Management Errors | ["CVE-2010-4756"] | ["CWE-399"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2018-20002"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2022-37454"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Resource Exhaustion | ["CVE-2018-15853"] | ["CWE-400"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Low | 150 | Divide By Zero | ["CVE-2021-20311"] | ["CWE-369"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2022-3213"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Reachable Assertion | ["CVE-2021-3326"] | ["CWE-617"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Information Exposure | ["CVE-2007-2768"] | ["CWE-200"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2021-4219"] | ["CWE-20"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2017-14974"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Incorrect Permission Assignment for Critical Resource | ["CVE-2018-7169"] | ["CWE-732"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-15938"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2018-6485"] | ["CWE-787"; "CWE-772"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-12433"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Improper Initialization | ["CVE-2017-14159"] | ["CWE-665"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Divide By Zero | ["CVE-2021-20241"] | ["CWE-369"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Link Following | ["CVE-2017-18078"] | ["CWE-59"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Divide By Zero | ["CVE-2021-20246"] | ["CWE-369"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-15225"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Double Free | ["CVE-2021-27645"] | ["CWE-415"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Incorrect Calculation of Buffer Size | ["CVE-2017-14934"] | ["CWE-131"; "CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2021-29921"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-12668"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2021-36087"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|--------------------|--------------------------------|--|------------------|------------------|-------------------------|----------------|
| Low | 150 | Incorrect Type Conversion or Cast | ["CVE-2017-9042"] | ["CWE-704"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Buffer Overflow | ["CVE-2019-8842"] | ["CWE-120"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2022-1304"] | ["CWE-125","CWE-732"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2022-1304"] | ["CWE-125","CWE-732"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2019-8907"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Memory Leak | ["CVE-2019-7398"] | ["CWE-401"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2018-16888"] | ["CWE-20","CWE-732","CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2017-16828"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2018-7568"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2018-19432"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2017-12452"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2019-17594"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2019-17594"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Low | 150 | Privilege Chaining | ["CVE-2019-3844"] | ["CWE-268"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Use of a Broken or Risky Cryptographic Algorithm | ["CVE-2018-6829"] | ["CWE-327"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Use of Externally-Controlled Format String | ["CVE-2021-35331"] | ["CWE-134"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Double Free | ["CVE-2018-6952"] | ["CWE-415"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Buffer Overflow | ["CVE-2021-4214"] | ["CWE-120"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2022-3219"] | ["CWE-787"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Information Exposure | ["CVE-2007-2768"] | ["CWE-200"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2021-35942"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2018-17966"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Allocation of Resources Without Limits or Throttling | ["CVE-2017-12132"] | ["CWE-770"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Allocation of Resources Without Limits or Throttling | ["CVE-2019-7148"] | ["CWE-770"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Allocation of Resources Without Limits or Throttling | ["CVE-2019-7148"] | ["CWE-770"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2017-17479"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-12675"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|----------------------|--------------------------------|--|------------------|------------------|-------------------------|----------------|
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-11644"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2018-6551"] | ["CWE-787","CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2021-39537"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Insufficiently Protected Credentials | ["CVE-2021-22923"] | ["CWE-522"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2017-8871"] | ["CWE-835"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Arbitrary Code Injection | ["CVE-2023-27533"] | ["CWE-74"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-21 16:47:40.962 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-14343"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-13059"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Improper Data Handling | ["CVE-2009-5155"] | ["CWE-19"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | Improper Data Handling | ["CVE-2009-5155"] | ["CWE-19"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | CVE-2020-14798 | ["CVE-2020-14798"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2020-35493"] | ["CWE-20","CWE-125","CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.449 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2022-29458"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2020-35521"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2019-9074"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.449 | Snyk Container |
| Low | 150 | Information Exposure | ["CVE-2019-1010024"] | ["CWE-200"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2016-9799"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Information Exposure | ["CVE-2022-0563"] | ["CWE-209"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Use of a Broken or Risky Cryptographic Algorithm | ["CVE-2018-6829"] | ["CWE-327"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | CVE-2020-2659 | ["CVE-2020-2659"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2016-9085"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Memory Leak | ["CVE-2019-6129"] | ["CWE-401"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | CVE-2020-2583 | ["CVE-2020-2583"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Use After Free | ["CVE-2018-20623"] | ["CWE-416"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Link Following | ["CVE-2013-4392"] | ["CWE-59"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2020-35495"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.449 | Snyk Container |
| Low | 150 | Information Exposure | ["CVE-2020-14145"] | ["CWE-200"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|--------------------|-----------------------|--|------------------|------------------|-------------------------|----------------|
| Low | 150 | CVE-2004-0971 | ["CVE-2004-0971"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.455 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2016-9580"] | ["CWE-190","CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Excessive Iteration | ["CVE-2018-11813"] | ["CWE-834"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2021-36690"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2018-10126"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Resource Exhaustion | ["CVE-2017-15298"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | CVE-2019-2962 | ["CVE-2019-2962"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2018-10126"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2019-16710"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2021-3575"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Buffer Overflow | ["CVE-2022-23219"] | ["CWE-120"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | Buffer Overflow | ["CVE-2022-23219"] | ["CWE-120"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-14139"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2016-2781"] | ["CWE-20"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Use of a Broken or Risky Cryptographic Algorithm | ["CVE-2019-14855"] | ["CWE-327"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Information Exposure | ["CVE-2021-33560"] | ["CWE-203"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Use After Free | ["CVE-2020-1752"] | ["CWE-416"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | CVE-2023-22607 | ["CVE-2023-22607"] | [] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2018-18700"] | ["CWE-835"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | CVE-2020-2590 | ["CVE-2020-2590"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Directory Traversal | ["CVE-2010-4651"] | ["CWE-22"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2018-17967"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Uncontrolled Recursion | ["CVE-2021-46195"] | ["CWE-674"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2017-7475"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Divide By Zero | ["CVE-2016-10506"] | ["CWE-369"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Arbitrary Command Injection | ["CVE-2015-20107"] | ["CWE-77"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2021-3826"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2016-8678"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|----------------------|-----------------------|--|------------------|------------------|-------------------------|----------------|
| Low | 150 | Out-of-bounds Write | ["CVE-2018-11490"] | ["CWE-787","CWE-287"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | Improper Authentication | ["CVE-2023-27538"] | ["CWE-287"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-21 16:47:40.962 | Snyk Container |
| Low | 150 | Improper Verification of Cryptographic Signature | ["CVE-2020-16156"] | ["CWE-347"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2019-9923"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | CVE-2022-42919 | ["CVE-2022-42919"] | [] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | CVE-2023-22605 | ["CVE-2023-22605"] | [] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-14326"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2017-13685"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2021-37600"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | CVE-2005-2541 | ["CVE-2005-2541"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Reachable Assertion | ["CVE-2019-6461"] | ["CWE-617"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Insufficiently Protected Credentials | ["CVE-2021-22923"] | ["CWE-522"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Cryptographic Issues | ["CVE-2010-0928"] | ["CWE-310"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2017-17080"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2022-48303"] | ["CWE-125"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | CVE-2019-2945 | ["CVE-2019-2945"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2022-27406"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2016-9801"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2016-9115"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-11755"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Memory Leak | ["CVE-2021-45346"] | ["CWE-401"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | CVE-2005-0406 | ["CVE-2005-0406"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Resource Exhaustion | ["CVE-2020-8492"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Improper Authentication | ["CVE-2021-36368"] | ["CWE-287"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Race Condition | ["CVE-2017-18018"] | ["CWE-362"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2021-40812"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2019-20386"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | CVE-2018-1000654 | ["CVE-2018-1000654"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|--------------------|------------------|--|------------------|------------------|-------------------------|----------------|
| Low | 150 | Out-of-Bounds | ["CVE-2016-9115"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Use After Free | ["CVE-2021-43400"] | ["CWE-416"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-9751"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-14324"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Resource Management Errors | ["CVE-2008-3134"] | ["CWE-399"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2017-2870"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2022-1304"] | ["CWE-125","CWE- | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Uncontrolled Recursion | ["CVE-2018-20796"] | ["CWE-674"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2018-15862"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Low | 150 | Cryptographic Issues | ["CVE-2013-7040"] | ["CWE-310"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2019-9075"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.449 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2016-2781"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | Uncontrolled Recursion | ["CVE-2020-12825"] | ["CWE-674"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Uncontrolled Recursion | ["CVE-2020-12825"] | ["CWE-674"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Use of Insufficiently Random Values | ["CVE-2015-9019"] | ["CWE-330"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2018-7642"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Resource Management Errors | ["CVE-2010-4756"] | ["CWE-399"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2017-14940"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2018-6485"] | ["CWE-787","CWE- | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-16232"] | ["CWE-772"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Release of Invalid Pointer or Reference | ["CVE-2021-45261"] | ["CWE-763"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2022-28506"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2019-16712"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2018-6551"] | ["CWE-787","CWE- | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2020-10029"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2020-10029"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-13131"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2017-5563"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|--------------------|-----------------------|--|------------------|------------------|-------------------------|----------------|
| Low | 150 | Out-of-Bounds | ["CVE-2017-7246"] | ["CWE-119"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Information Exposure | ["CVE-2021-3426"] | ["CWE-200"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Arbitrary Command Injection | ["CVE-2015-20107"] | ["CWE-77"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | CVE-2018-6954 | ["CVE-2018-6954"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-7246"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-14729"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2020-12062"] | ["CWE-20"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2021-29921"] | ["CWE-20"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Off-by-one Error | ["CVE-2022-3821"] | ["CWE-193"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Release of Invalid Pointer or Reference | ["CVE-2021-45261"] | ["CWE-763"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Cryptographic Issues | ["CVE-2007-6755"] | ["CWE-310"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Memory Leak | ["CVE-2019-7395"] | ["CWE-401"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2021-20298"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2016-9580"] | ["CWE-190","CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-12642"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Resource Management Errors | ["CVE-2007-3477"] | ["CWE-399"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | CVE-2021-40330 | ["CVE-2021-40330"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-9742"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2017-6311"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Open Redirect | ["CVE-2021-28861"] | ["CWE-601"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Incorrect Permission Assignment for Critical Resource | ["CVE-2019-19882"] | ["CWE-732"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2018-17360"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2020-27618"] | ["CWE-835"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2018-10534"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2018-18661"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-17882"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Use After Free | ["CVE-2018-20623"] | ["CWE-416"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2018-19211"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|--------------------|-------------|--|------------------|------------------|-------------------------|----------------|
| Low | 150 | NULL Pointer Dereference | ["CVE-2018-19211"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Incorrect Type Conversion or Cast | ["CVE-2022-32547"] | ["CWE-704"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2017-15024"] | ["CWE-835"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2014-8166"] | ["CWE-20"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2022-1056"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Authentication Bypass | ["CVE-2020-13529"] | ["CWE-290"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Allocation of Resources Without Limits or Throttling | ["CVE-2017-13716"] | ["CWE-770"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2018-13139"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2022-31782"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Improper Authentication | ["CVE-2007-2243"] | ["CWE-287"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Uncontrolled Recursion | ["CVE-2019-9192"] | ["CWE-674"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-17124"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | CVE-2021-35588 | ["CVE-2021-35588"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Low | 150 | Divide By Zero | ["CVE-2021-20243"] | ["CWE-369"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2016-3977"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2019-17451"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Memory Leak | ["CVE-2021-40633"] | ["CWE-401"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | Insufficiently Protected Credentials | ["CVE-2021-22923"] | ["CWE-522"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2018-16376"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2019-20838"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Reachable Assertion | ["CVE-2021-3326"] | ["CWE-617"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | Cryptographic Issues | ["CVE-2007-6755"] | ["CWE-310"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2019-8457"] | ["CWE-125"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2019-8457"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2016-9802"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Information Exposure | ["CVE-2018-16868"] | ["CWE-203"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2017-12618"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.449 | Snyk Container |
| Low | 150 | Incorrect Permission Assignment for Critical Resource | ["CVE-2019-19882"] | ["CWE-732"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|--------------------|-------------|--|------------------|------------------|-------------------------|----------------|
| Low | 150 | NULL Pointer Dereference | ["CVE-2021-4217"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.457 | Snyk Container |
| Low | 150 | CVE-2018-14048 | ["CVE-2018-14048"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Link Following | ["CVE-2017-18078"] | ["CWE-59"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-17740"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2019-9077"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.449 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2021-4219"] | ["CWE-20"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Race Condition | ["CVE-2017-18018"] | ["CWE-362"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | Memory Leak | ["CVE-2020-27755"] | ["CWE-401"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-9755"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2019-7149"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | CVE-2019-2964 | ["CVE-2019-2964"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-11697"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2018-11656"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2017-6363"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Information Exposure | ["CVE-2020-14145"] | ["CWE-200"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2021-4217"] | ["CWE-476"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-16231"] | ["CWE-119"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | CVE-2004-0971 | ["CVE-2004-0971"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2021-20312"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Improper Validation of Integrity Check Value | ["CVE-2021-22922"] | ["CWE-354"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | Exposure of Resource to Wrong Sphere | ["CVE-2022-24975"] | ["CWE-668"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Excessive Iteration | ["CVE-2018-11813"] | ["CWE-834"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2021-36690"] | ["CWE-125"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Resource Exhaustion | ["CVE-2019-9674"] | ["CWE-400"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2019-8457"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2016-9113"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2022-3219"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Improper Authentication | ["CVE-2021-36368"] | ["CWE-287"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|----------------------|-----------------------|--|------------------|------------------|-------------------------|----------------|
| Low | 150 | NULL Pointer Dereference | ["CVE-2018-7999"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2018-1000030"] | ["CWE-787","CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-14325"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2018-17358"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2019-17595"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Low | 150 | Information Exposure | ["CVE-2018-15919"] | ["CWE-200"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Memory Leak | ["CVE-2019-7397"] | ["CWE-401"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | CVE-2020-14581 | ["CVE-2020-14581"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-12662"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2017-1000082"] | ["CWE-20"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2018-18064"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2019-11023"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Race Condition | ["CVE-2017-18018"] | ["CWE-362"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Information Exposure | ["CVE-2019-1010024"] | ["CWE-200"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Memory Leak | ["CVE-2021-3574"] | ["CWE-401"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2020-36135"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2018-14553"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2019-1010022"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2019-1010022"] | ["CWE-119"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Divide By Zero | ["CVE-2021-20244"] | ["CWE-369"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Incorrect Authorization | ["CVE-2021-3658"] | ["CWE-863"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Cross-site Request Forgery (CSRF) | ["CVE-2018-1000858"] | ["CWE-352"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Cryptographic Issues | ["CVE-2010-0928"] | ["CWE-310"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-18029"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2020-14155"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2019-9070"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.449 | Snyk Container |
| Low | 150 | CVE-2019-2894 | ["CVE-2019-2894"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Allocation of Resources Without Limits or Throttling | ["CVE-2020-25648"] | ["CWE-770"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|---------------------|-----------------------------------|--|------------------|------------------|-------------------------|----------------|
| Low | 150 | Improper Certificate Validation | ["CVE-2020-15719"] | ["CWE-295"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Improper Certificate Validation | ["CVE-2020-15719"] | ["CWE-295"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | CVE-2019-2786 | ["CVE-2019-2786"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Arbitrary Code Injection | ["CVE-2019-18348"] | ["CWE-74"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | CVE-2020-27619 | ["CVE-2020-27619"] | [] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2018-6405"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Off-by-one Error | ["CVE-2021-3999"] | ["CWE-193"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2018-10372"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2019-0053"] | ["CWE-787", "CWE-327", "CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Use of a Broken or Risky Cryptographic Algorithm | ["CVE-2019-1563"] | ["CWE-327", "CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2022-48303"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-17887"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2018-12699"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2022-27406"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | Access Restriction Bypass | ["CVE-2007-5686"] | ["CWE-264"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2018-18483"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2017-12967"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2018-100021"] | ["CWE-20"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2019-20386"] | ["CWE-772"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Improper Certificate Validation | ["CVE-2023-0464"] | ["CWE-295"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-23 18:46:28.727 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2019-25013"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-11696"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Low | 150 | Improper Authentication | ["CVE-2023-27535"] | ["CWE-287"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-21 18:40:28.583 | Snyk Container |
| Low | 150 | Resource Exhaustion | ["CVE-2022-4899"] | ["CWE-400"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-04-04 21:11:00.928 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2022-1115"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2017-16831"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2017-2870"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | Loop with Unreachable Exit Condition ('Infinite Loop') | ["CVE-2017-14932"] | ["CWE-835"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|--------------------|-----------------------|--|------------------|------------------|-------------------------|----------------|
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-12565"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2022-1304"] | ["CWE-125","CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-9750"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2017-17123"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2021-36087"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2021-36087"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2017-12454"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Memory Leak | ["CVE-2021-45346"] | ["CWE-401"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Memory Leak | ["CVE-2019-13137"] | ["CWE-401"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | CVE-2020-14797 | ["CVE-2020-14797"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Low | 150 | Use After Free | ["CVE-2021-36084"] | ["CWE-416"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Arbitrary Code Injection | ["CVE-2017-17522"] | ["CWE-74"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2017-14130"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Use After Free | ["CVE-2017-12448"] | ["CWE-416"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2022-37454"] | ["CWE-190"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Arbitrary Code Injection | ["CVE-2022-0391"] | ["CWE-74"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | CVE-2022-39177 | ["CVE-2022-39177"] | [] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2018-15854"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-15088"] | ["CWE-119","CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Resource Management Errors | ["CVE-2010-4756"] | ["CWE-399"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Information Exposure | ["CVE-2018-16868"] | ["CWE-203"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2019-16711"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | CVE-2018-3139 | ["CVE-2018-3139"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Uncontrolled Recursion | ["CVE-2018-9138"] | ["CWE-674"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Incorrect Privilege Assignment | ["CVE-2019-3843"] | ["CWE-266"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | CVE-2018-14048 | ["CVE-2018-14048"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2022-4285"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Allocation of Resources Without Limits or Throttling | ["CVE-2018-12934"] | ["CWE-770"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|---|--------------------|----------------------|--|------------------|------------------|-------------------------|----------------|
| Low | 150 | Out-of-bounds Write | ["CVE-2018-16375"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Cryptographic Issues | ["CVE-2015-3276"] | ["CWE-310"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Improper Data Handling | ["CVE-2015-8985"] | ["CWE-19"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2017-12670"] | ["CWE-20","CWE-617"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Off-by-one Error | ["CVE-2022-3821"] | ["CWE-193"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-7275"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Uncontrolled Recursion | ["CVE-2017-11164"] | ["CWE-674"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2017-15020"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Numeric Errors | ["CVE-2007-3476"] | ["CWE-189"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Incorrect Permission Assignment for Critical Resource | ["CVE-2019-5068"] | ["CWE-732"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-13146"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Allocation of Resources Without Limits or Throttling | ["CVE-2017-14531"] | ["CWE-770"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | CVE-2008-1687 | ["CVE-2008-1687"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Open Redirect | ["CVE-2021-28861"] | ["CWE-601"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-17121"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2016-10713"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Exposure of Resource to Wrong Sphere | ["CVE-2022-24975"] | ["CWE-668"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Improper Authentication | ["CVE-2023-27536"] | ["CWE-287"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-21 16:47:40.962 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2017-5563"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2021-46822"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Divide By Zero | ["CVE-2014-8130"] | ["CWE-369"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2018-5727"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Authentication Bypass | ["CVE-2020-13529"] | ["CWE-290"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2018-6872"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Divide By Zero | ["CVE-2017-15025"] | ["CWE-369"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Use After Free | ["CVE-2021-33574"] | ["CWE-416"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | Use After Free | ["CVE-2021-33574"] | ["CWE-416"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-11539"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|--------------------|-------------|--|------------------|------------------|-------------------------|----------------|
| Low | 150 | Uncontrolled Recursion | ["CVE-2018-20796"] | ["CWE-674"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Uncontrolled Recursion | ["CVE-2018-20796"] | ["CWE-674"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | Information Exposure | ["CVE-2018-15919"] | ["CWE-200"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-16231"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-12427"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2020-16593"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.449 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2016-9918"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.324 | Snyk Container |
| Low | 150 | Use After Free | ["CVE-2020-1752"] | ["CWE-416"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | CVE-2019-2978 | ["CVE-2019-2978"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2018-10126"] | ["CWE-476"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Arbitrary Code Injection | ["CVE-2023-27533"] | ["CWE-74"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-21 18:40:28.583 | Snyk Container |
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-17885"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | NULL Pointer Dereference | ["CVE-2016-9116"] | ["CWE-476"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2018-5709"] | ["CWE-190"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.668 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2019-17543"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2017-5563"] | ["CWE-125"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-7246"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Out-of-bounds Read | ["CVE-2017-14129"] | ["CWE-125"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Information Exposure | ["CVE-2021-3426"] | ["CWE-200"] | e-corp-demo/java-goof(main):log4shell-goof/log4shell-server/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:08.200 | Snyk Container |
| Low | 150 | CVE-2020-14579 | ["CVE-2020-14579"] | [] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.670 | Snyk Container |
| Low | 150 | CVE-2018-6954 | ["CVE-2018-6954"] | [] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.456 | Snyk Container |
| Low | 150 | XML External Entity (XXE) Injection | ["CVE-2013-0340"] | ["CWE-611"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | Integer Overflow or Wraparound | ["CVE-2018-5709"] | ["CWE-190"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.455 | Snyk Container |
| Low | 150 | Resource Exhaustion | ["CVE-2017-14988"] | ["CWE-400"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:11.325 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-9754"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2019-12900"] | ["CWE-787"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Out-of-bounds Write | ["CVE-2019-12900"] | ["CWE-787"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.667 | Snyk Container |
| Low | 150 | Improper Certificate Validation | ["CVE-2023-0466"] | ["CWE-295"] | e-corp-demo/java-goof(main):todolist-goof/exploits/tomcat-rce/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-29 22:23:50.983 | Snyk Container |

| Severity | Prio | Title | CVE | CWE | Project Name | Exploit Maturity | Autofixable | First Introduction | Product |
|----------|------|--|--------------------|-------------|--|------------------|------------------|-------------------------|----------------|
| Low | 150 | Missing Release of Resource after Effective Lifetime | ["CVE-2017-12566"] | ["CWE-772"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.451 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-9746"] | ["CWE-119"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |
| Low | 150 | Cross-site Scripting (XSS) | ["CVE-2018-18405"] | ["CWE-79"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.455 | Snyk Container |
| Low | 150 | Out-of-Bounds | ["CVE-2017-11698"] | ["CWE-119"] | e-corp-demo/java-goof(main):todolist-goof/Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 21:11:12.669 | Snyk Container |
| Low | 150 | Improper Input Validation | ["CVE-2018-6759"] | ["CWE-20"] | e-corp-demo/goof-kubernetes(master):Dockerfile | No Known Exploit | Not Auto Fixable | 2023-03-07 23:04:19.450 | Snyk Container |