

DevOps World



Jenkins World

Sysdig Secure Jenkins Plugin

By Marky Jackson



Who Is Marky

- Jenkins Contributor
- Kubernetes Org Member
- Sysdig Software Engineer



Who is Sysdig

Sysdig is the first unified cloud-native visability + security platform



Docker scanning for Jenkins

CI/CD security with the sysdig secure plugin



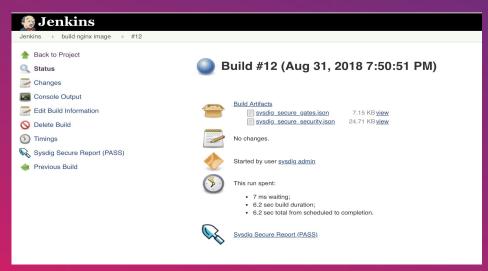
Scanning docker images built with Jenkins

Configure the plugin to integrate with sysdig secure

Engine Mode		0
Engine URL	https://secure.sysdig.com/api/scanning/v1/anchore	0
Sysdig Secure API Token	API token	0
Verify SSL		
Enable DEBUG logging		0

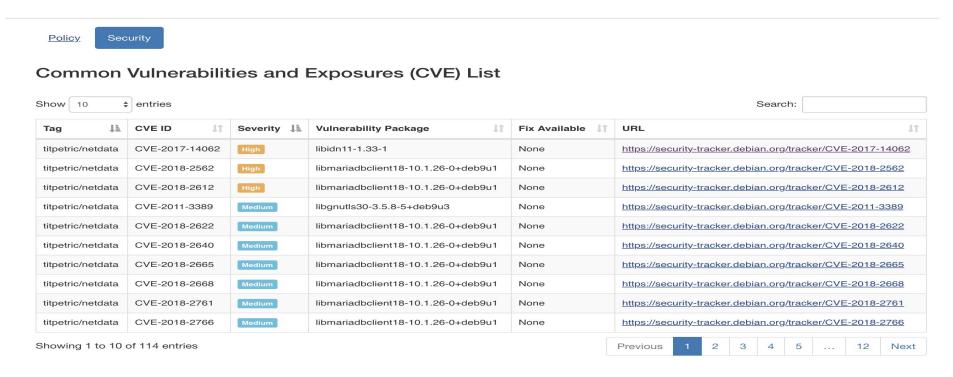


Scanning docker images as part of the CI/CD pipeline with Jenkins



Review the Report

 By clicking into the Sysdig Secure Report you'll get a summary of the policy evaluation broken down by the different stop or warn actions that were generated from the policy



Console Output

```
ction", "Dockerfile directive 'HEALTHCHECK' not found, matching condition 'not exists' check", "warn", false, "default"],
["380b0abb8bfdefedeae4d5b04de2059c1b7d0159e0bb3bfc38e204ea313a1dc8", "docker.io/sysdig/agent:dev", "CVE-2018-
10372+binutils", "vulnerabilities", "package", "MEDIUM Vulnerability found in os package type (dpkg) - binutils (CVE-2018-10372 - https://security-
tracker.debian.org/tracker/CVE-2018-10372)","warn",false,"default"],
["380b0abb8bfdefedeae4d5b04de2059c1b7d0159e0bb3bfc38e204ea313a1dc8", "docker.io/sysdig/agent:dev", "CVE-2018-
10373+binutils", "vulnerabilities", "package", "MEDIUM Vulnerability found in os package type (dpkg) - binutils (CVE-2018-10373 - https://security-
tracker.debian.org/tracker/CVE-2018-10373)","warn",false,"default"],
["380b0abb8bfdefedeae4d5b04de2059c1b7d0159e0bb3bfc38e204ea313a1dc8", "docker.io/sysdig/agent:dev", "CVE-2018-
10534+binutils", "vulnerabilities", "package", "MEDIUM Vulnerability found in os package type (dpkg) - binutils (CVE-2018-10534 - https://security-
tracker.debian.org/tracker/CVE-2018-10534)", "warn", false, "default"],
["380b0abb8bfdefedeae4d5b04de2059c1b7d0159e0bb3bfc38e204ea313a1dc8", "docker.io/sysdig/agent:dev", "CVE-2018-
10535+binutils", "vulnerabilities", "package", "MEDIUM Vulnerability found in os package type (dpkg) - binutils (CVE-2018-10535 - https://security-
tracker.debian.org/tracker/CVE-2018-10535) ", "warn", false, "default" ],
["380b0abb8bfdefedeae4d5b04de2059c1b7d0159e0bb3bfc38e204ea313a1dc8","docker.io/sysdig/agent:dev","CVE-2018-10372+binutils-
common", "vulnerabilities", "package", "MEDIUM Vulnerability found in os package type (dpkg) - binutils-common (CVE-2018-10372 - https://security-
tracker.debian.org/tracker/CVE-2018-10372)", "warn", false, "default"],
["380b0abb8bfdefedeae4d5b04de2059c1b7d0159e0bb3bfc38e204ea313a1dc8", "docker.io/sysdig/agent:dev", "CVE-2018-10373+binutils-
common", "vulnerabilities", "package", "MEDIUM Vulnerability found in os package type (dpkg) - binutils-common (CVE-2018-10373 - https://security-
tracker.debian.org/tracker/CVE-2018-10373)", "warn", false, "default"],
["380b0abb8bfdefedeae4d5b04de2059c1b7d0159e0bb3bfc38e204ea313a1dc8", "docker.io/sysdig/agent:dev", "CVE-2018-10534+binutils-
common", "vulnerabilities", "package", "MEDIUM Vulnerability found in os package type (dpkg) - binutils-common (CVE-2018-10534 - https://security-
tracker.debian.org/tracker/CVE-2018-10534)", "warn", false, "default"],
["380b0abb8bfdefedeae4d5b04de2059c1b7d0159e0bb3bfc38e204ea313a1dc8","docker.io/sysdig/agent:dev","CVE-2018-10535+binutils-
common", "vulnerabilities", "package", "MEDIUM Vulnerability found in os package type (dpkg) - binutils-common (CVE-2018-10535 - https://security-
tracker.debian.org/tracker/CVE-2018-10535)","warn",false,"default"],
["380b0abb8bfdefedeae4d5b04de2059c1b7d0159e0bb3bfc38e204ea313a1dc8", "docker.io/sysdig/agent:dev", "CVE-2018-10372+binutils-x86-64-linux-
gnu", "vulnerabilities", "package", "MEDIUM Vulnerability found in os package type (dpkg) - binutils-x86-64-linux-gnu (CVE-2018-10372 - https://security-
tracker.debian.org/tracker/CVE-2018-10372)","warn",false,"default"],
```

Lets try a demo



Tying It All Together

All this data is also sent to the Sysdig Secure UI where you can get further details about the

- Image
- OS package information
- Configuration files
- Discovered vulnerabilities
- Any possible leaked secrets or credentials
- A view into if & where this image is currently running in your environment

Where Can I Learn More

- https://sysdig.com
- Our github repository:
 https://github.com/jenkinsci/sysdig-secure-plugin
- At our booth #1132
- On Gitter

