



DevOps World



Jenkins World

Sysdig Secure Jenkins Plugin

By Marky Jackson





Community
Lunch Time
Demos

Who Is Marky

- Jenkins Contributor
- Kubernetes Org Member
- Sysdig Software Engineer



Community
Lunch Time
Demos

Who is Sysdig

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



Community
Lunch Time
Demos

Docker scanning for Jenkins

CI/CD security with the sysdig
secure plugin



Community
Lunch Time
Demos

Scanning docker images built with Jenkins

Configure the plugin to integrate
with sysdig secure

Sysdig Secure Plugin Mode

☒ Engine Mode

Engine URL

Sysdig Secure API Token

Verify SSL ☒

Enable DEBUG logging ☐



Community
Lunch Time
Demos

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

Jenkins

Jenkins » build nginx image » #12

Back to Project
Status
Changes
Console Output
Edit Build Information
Delete Build
Timings
Sysdig Secure Report (PASS)
Previous Build

Build #12 (Aug 31, 2018 7:50:51 PM)

Build Artifacts

Artifact	Size	View
sysdig_secure_gates.json	7.15 KB	view
sysdig_secure_security.json	24.71 KB	view

No changes.

Started by user [sysdig_admin](#)

This run spent:

- 7 ms waiting;
- 6.2 sec build duration;
- 6.2 sec total from scheduled to completion.

[Sysdig Secure Report \(PASS\)](#)

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

[Policy](#) [Security](#)

Common Vulnerabilities and Exposures (CVE) List

Show entries Search:

Tag	CVE ID	Severity	Vulnerability Package	Fix Available	URL
titpetric/netdata	CVE-2017-14062	High	libidn11-1.33-1	None	https://security-tracker.debian.org/tracker/CVE-2017-14062
titpetric/netdata	CVE-2018-2562	High	libmariadbclient18-10.1.26-0+deb9u1	None	https://security-tracker.debian.org/tracker/CVE-2018-2562
titpetric/netdata	CVE-2018-2612	High	libmariadbclient18-10.1.26-0+deb9u1	None	https://security-tracker.debian.org/tracker/CVE-2018-2612
titpetric/netdata	CVE-2011-3389	Medium	libgnutls30-3.5.8-5+deb9u3	None	https://security-tracker.debian.org/tracker/CVE-2011-3389
titpetric/netdata	CVE-2018-2622	Medium	libmariadbclient18-10.1.26-0+deb9u1	None	https://security-tracker.debian.org/tracker/CVE-2018-2622
titpetric/netdata	CVE-2018-2640	Medium	libmariadbclient18-10.1.26-0+deb9u1	None	https://security-tracker.debian.org/tracker/CVE-2018-2640
titpetric/netdata	CVE-2018-2665	Medium	libmariadbclient18-10.1.26-0+deb9u1	None	https://security-tracker.debian.org/tracker/CVE-2018-2665
titpetric/netdata	CVE-2018-2668	Medium	libmariadbclient18-10.1.26-0+deb9u1	None	https://security-tracker.debian.org/tracker/CVE-2018-2668
titpetric/netdata	CVE-2018-2761	Medium	libmariadbclient18-10.1.26-0+deb9u1	None	https://security-tracker.debian.org/tracker/CVE-2018-2761
titpetric/netdata	CVE-2018-2766	Medium	libmariadbclient18-10.1.26-0+deb9u1	None	https://security-tracker.debian.org/tracker/CVE-2018-2766

Showing 1 to 10 of 114 entries

[Previous](#) [1](#) [2](#) [3](#) [4](#) [5](#) [...](#) [12](#) [Next](#)

Console Output

```

ction", "Dockerfile directive 'HEALTHCHECK' not found, matching condition 'not_exists' check", "warn", false, "default"],
["380b0abb8bfdefedea4d5b04de2059c1b7d0159e0bb3bfc38e204ea313a1dc8", "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"].
["380b0abb8bfdefedea4d5b04de2059c1b7d0159e0bb3bfc38e204ea313a1dc8", "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"].
["380b0abb8bfdefedea4d5b04de2059c1b7d0159e0bb3bfc38e204ea313a1dc8", "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"].
["380b0abb8bfdefedea4d5b04de2059c1b7d0159e0bb3bfc38e204ea313a1dc8", "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"].
["380b0abb8bfdefedea4d5b04de2059c1b7d0159e0bb3bfc38e204ea313a1dc8", "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"].
["380b0abb8bfdefedea4d5b04de2059c1b7d0159e0bb3bfc38e204ea313a1dc8", "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"].
["380b0abb8bfdefedea4d5b04de2059c1b7d0159e0bb3bfc38e204ea313a1dc8", "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"].
["380b0abb8bfdefedea4d5b04de2059c1b7d0159e0bb3bfc38e204ea313a1dc8", "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"].
["380b0abb8bfdefedea4d5b04de2059c1b7d0159e0bb3bfc38e204ea313a1dc8", "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"].
["380b0abb8bfdefedea4d5b04de2059c1b7d0159e0bb3bfc38e204ea313a1dc8", "docker.io/sysdig/agent:dev", "CVE-2018-10373+binutils-x86-64-linux-gnu", "vulnerabilities", "package", "MEDIUM Vulnerability found in os package type (dpkg) - binutils-x86-64-linux-gnu (CVE-2018-10373 - https://security-tracker.debian.org/tracker/CVE-2018-10373)", "warn", false, "default"].
["380b0abb8bfdefedea4d5b04de2059c1b7d0159e0bb3bfc38e204ea313a1dc8", "docker.io/sysdig/agent:dev", "CVE-2018-10534+binutils-x86-64-linux-gnu", "vulnerabilities", "package", "MEDIUM Vulnerability found in os package type (dpkg) - binutils-x86-64-linux-gnu (CVE-2018-10534 - https://security-tracker.debian.org/tracker/CVE-2018-10534)", "warn", false, "default"].
["380b0abb8bfdefedea4d5b04de2059c1b7d0159e0bb3bfc38e204ea313a1dc8", "docker.io/sysdig/agent:dev", "CVE-2018-10535+binutils-x86-64-linux-gnu", "vulnerabilities", "package", "MEDIUM Vulnerability found in os package type (dpkg) - binutils-x86-64-linux-gnu (CVE-2018-10535 - https://security-tracker.debian.org/tracker/CVE-2018-10535)", "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

DevOps World



Jenkins World

Thank You

