Best OS-Based Image for Hosting Nginx with Minimal Vulnerabilities

Reference:
Vulnerability Analysis of Docker Hub Official Images and Verified Images

It shows the major Docker image vulnerabilities using different scanning tools including Trivy. In our data below, we have scanned OS-based images to address and find the best OS-based image to host Nginx with fewer vulnerabilities and issues.

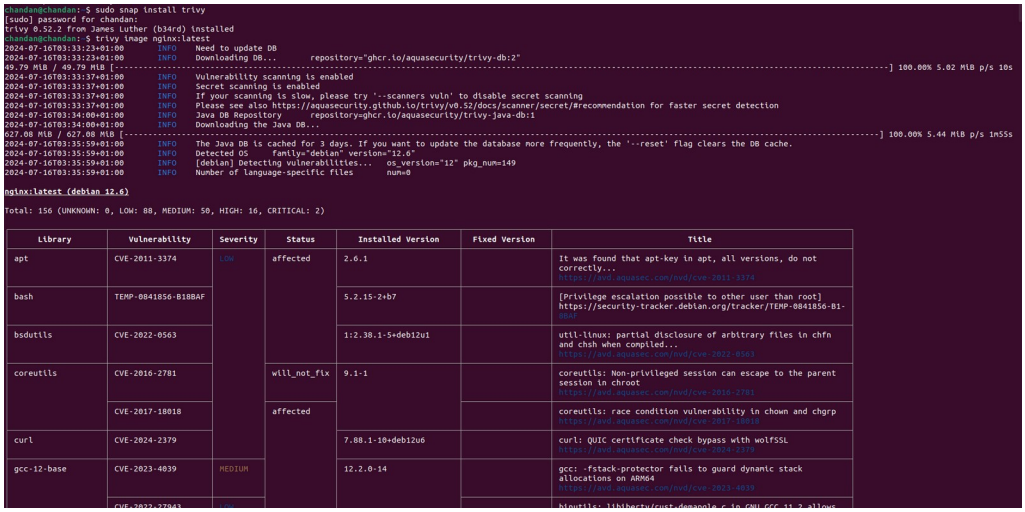
https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10254755

To secure a Docker-based image of the official and verified Nginx image, we need to analyze the Docker Hub official image as the first line of security.

- **What tools can be integrated, and how can we analyze the image to ensure that the base image is secure for hosting Nginx on it?**

To secure a Docker-based image of the official and verified Nginx image from Docker Hub, you can integrate various tools to analyze and ensure the security of the base image. Here are the steps and tools you can use:

1. **Static Analysis of Docker Image**:
    - **Trivy**: A comprehensive vulnerability scanner for containers and other artifacts. It scans for vulnerabilities, misconfigurations, and secrets in Docker images.



Analyze the best OS to host Nginx on top of that.

Result 1 : Offical Ubuntu Image

ubuntu:latest (ubuntu 24.04)
Total: 9 (UNKNOWN: 0, LOW: 7, MEDIUM: 2, HIGH: 0, CRITICAL: 0)

```
chandan@chandan:~$ trivy image ubuntu:latest
2024-07-16T03:50:26+01:00	INFO	Vulnerability scanning is enabled
2024-07-16T03:50:26+01:00	INFO	Secret scanning is enabled
2024-07-16T03:50:26+01:00	INFO	If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2024-07-16T03:50:26+01:00	INFO	Please see also https://aquasecurity.github.io/trivy/v0.52/docs/scanner/secret/#recommendation for faster secret detection
2024-07-16T03:50:40+01:00	INFO	Detected OS	family="ubuntu" version="24.04"
2024-07-16T03:50:40+01:00	INFO	[ubuntu] Detecting vulnerabilities...	os_version="24.04" pkg_num=91
2024-07-16T03:50:40+01:00	INFO	Number of language-specific files	num=0

ubuntu:latest (ubuntu 24.04)

Total: 9 (UNKNOWN: 0, LOW: 7, MEDIUM: 2, HIGH: 0, CRITICAL: 0)
```

Library	Vulnerability	Severity	Status	Installed Version	Fixed Version	Title
coreutils	CVE-2016-2781	LOW	affected	9.4-3ubuntu6		coreutils: Non-privileged session can escape to the parent session in chroot https://avd.aquasec.com/nvd/cve-2016-2781
gpgv	CVE-2022-3219			2.4.4-2ubuntu17		gnupg: denial of service issue (resource consumption) using compressed packets https://avd.aquasec.com/nvd/cve-2022-3219
libc-bin	CVE-2016-20013			2.39-0ubuntu8.2		sha256crypt and sha512crypt through 0.6 allow attackers to cause a denial of... https://avd.aquasec.com/nvd/cve-2016-20013
libc6						
libgcrypt20	CVE-2024-2236	MEDIUM		1.10.3-2build1		libgcrypt: vulnerable to Marvin Attack https://avd.aquasec.com/nvd/cve-2024-2236
liblzma5	CVE-2020-22916			5.6.1+really5.4.5-1		Denial of service via decompression of crafted file https://avd.aquasec.com/nvd/cve-2020-22916
libssl3t64	CVE-2024-2511	LOW		3.0.13-0ubuntu3.1		openssl: Unbounded memory growth with session handling in TLSv1.3 https://avd.aquasec.com/nvd/cve-2024-2511
	CVE-2024-4603					openssl: Excessive time spent checking DSA keys and parameters https://avd.aquasec.com/nvd/cve-2024-4603
	CVE-2024-4741					openssl: Use After Free with SSL_free_buffers https://avd.aquasec.com/nvd/cve-2024-4741

Result 2 : Offical Alpine Image

alpine:latest (alpine 3.20.1)

Total: 2 (UNKNOWN: 0, LOW: 0, MEDIUM: 2, HIGH: 0, CRITICAL: 0)

```
chandan@chandan:~$ trivy image alpine:latest
2024-07-16T04:14:52+01:00	INFO	Vulnerability scanning is enabled
2024-07-16T04:14:52+01:00	INFO	Secret scanning is enabled
2024-07-16T04:14:52+01:00	INFO	If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2024-07-16T04:14:52+01:00	INFO	Please see also https://aquasecurity.github.io/trivy/v0.52/docs/scanner/secret/#recommendation for faster secret detection
2024-07-16T04:14:57+01:00	INFO	Detected OS	family="alpine" version="3.20.1"
2024-07-16T04:14:57+01:00	INFO	[alpine] Detecting vulnerabilities...	os_version="3.20" repository="3.20" pkg_num=14
2024-07-16T04:14:57+01:00	INFO	Number of language-specific files	num=0

alpine:latest (alpine 3.20.1)

Total: 2 (UNKNOWN: 0, LOW: 0, MEDIUM: 2, HIGH: 0, CRITICAL: 0)
```

Library	Vulnerability	Severity	Status	Installed Version	Fixed Version	Title
libcrypto3	CVE-2024-5535	MEDIUM	fixed	3.3.1-r0	3.3.1-r1	openssl: SSL_select_next_proto buffer overread https://avd.aquasec.com/nvd/cve-2024-5535
libssl3						

Result 2 : Offical debian Image

debian:latest (debian 12.6)

Total: 72 (UNKNOWN: 0, LOW: 57, MEDIUM: 13, HIGH: 1, CRITICAL: 1)

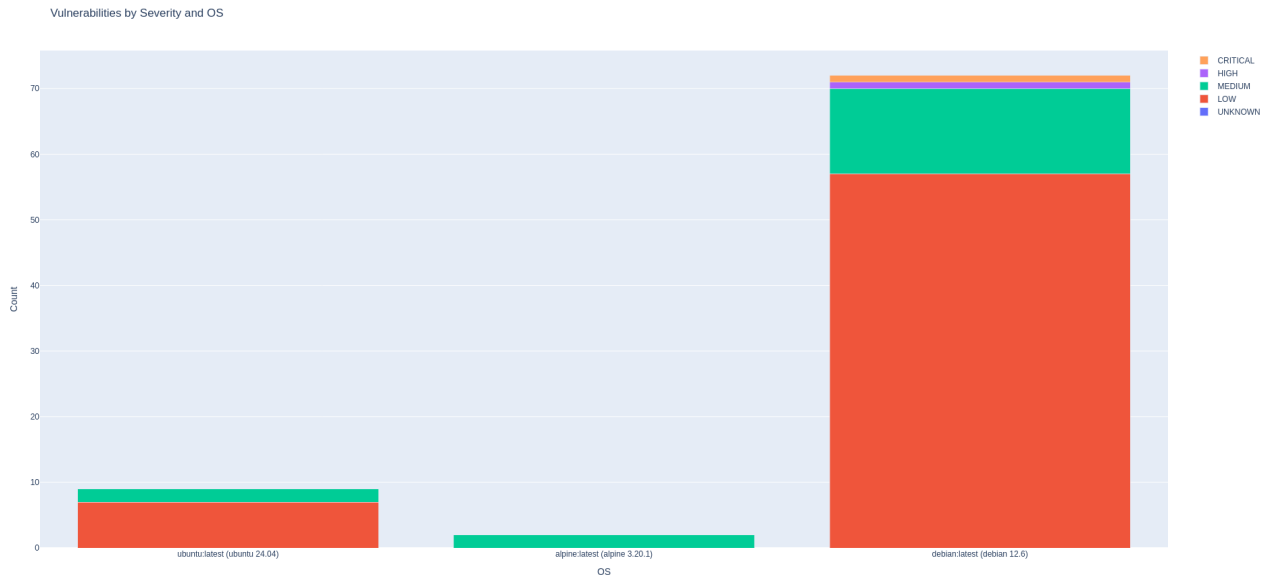
```
chandan@chandan:~$ trivy image debian:latest
2024-07-16T04:17:28+01:00	INFO	Vulnerability scanning is enabled
2024-07-16T04:17:28+01:00	INFO	Secret scanning is enabled
2024-07-16T04:17:28+01:00	INFO	If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2024-07-16T04:17:28+01:00	INFO	Please see also https://aquasecurity.github.io/trivy/v0.52/docs/scanner/secret/#recommendation for faster secret detection
2024-07-16T04:17:41+01:00	INFO	Detected OS	family="debian" version="12.6"
2024-07-16T04:17:41+01:00	INFO	[debian] Detecting vulnerabilities...	os_version="12" pkg_num=88
2024-07-16T04:17:41+01:00	INFO	Number of language-specific files	num=0

debian:latest (debian 12.6)

Total: 72 (UNKNOWN: 0, LOW: 57, MEDIUM: 13, HIGH: 1, CRITICAL: 1)
```

Library	Vulnerability	Severity	Status	Installed Version	Fixed Version	Title
apt	CVE-2011-3374	LOW	affected	2.6.1		It was found that apt-key in apt, all versions, do not correctly... https://avd.aquasec.com/nvd/cve-2011-3374
bash	TEMP-0841856-B18BAF			5.2.15-2+b7		[Privilege escalation possible to other user than root] https://security-tracker.debian.org/tracker/TEMP-0841856-B1-8BAF
bsdutils	CVE-2022-0563			1:2.38.1-5+deb12u1		util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled... https://avd.aquasec.com/nvd/cve-2022-0563
coreutils	CVE-2016-2781		will_not_fix	9.1-1		coreutils: Non-privileged session can escape to the parent session in chroot https://avd.aquasec.com/nvd/cve-2016-2781
	CVE-2017-18018		affected			coreutils: race condition vulnerability in chown and chgrp https://avd.aquasec.com/nvd/cve-2017-18018
gcc-12-base	CVE-2023-4039	MEDIUM		12.2.0-14		gcc: -fstack-protector fails to guard dynamic stack allocations on ARM64 https://avd.aquasec.com/nvd/cve-2023-4039
	CVE-2022-27943	LOW				binutils: libiberty/rust-demangle.c in GNU GCC 11.2 allows stack exhaustion in demangle_const https://avd.aquasec.com/nvd/cve-2022-27943

Comparison of all the Trivy results in a bar chart representation.



The results show a comparison of three major OS images in Docker. Alpine has the fewest vulnerabilities and is the best practice to use for deploying Nginx.