

Stop Chasing CVEs

nemo | Oct 2024

Mercari India Security Conclave

About Me

Founding Engineer @ Razorpay

Creator, endoflife.date

OSS Maintainer

captnemo.in | blr.today

Recurse Center Alum

Takshashila Scholar

Speedcuber, Homelabber, Niradhaar



endoflife.date

Kubernetes

SERVER-APP

Last updated on 12 September 2024



Kubernetes is an open-source container-orchestration system for automating computer application deployment, scaling, and management.

Release	Released	Active Support	Maintenance Support	Latest
1.31	1 month and 3 weeks ago (13 Aug 2024)	Ends in 10 months (28 Aug 2025)	Ends in 1 year (28 Oct 2025)	1.31.1 (11 Sep 2024)
1.30	5 months and 2 weeks ago (17 Apr 2024)	Ends in 6 months and 3 weeks (28 Apr 2025)	Ends in 8 months and 3 weeks (28 Jun 2025)	1.30.5 (12 Sep 2024)
1.29	9 months ago (13 Dec 2023)	Ends in 2 months and 3 weeks (28 Dec 2024)	Ends in 4 months and 3 weeks (28 Feb 2025)	1.29.9 (11 Sep 2024)
1.28	1 year and 1 month ago (15 Aug 2023)	Ended 1 month and 1 week ago (28 Aug 2024)	Ends in 3 weeks and 3 days (28 Oct 2024)	1.28.14 (11 Sep 2024)
1.27	1 year and 5 months ago (11 Apr 2023)	Ended 5 months ago (28 Apr 2024)	Ended 3 months ago (28 Jun 2024)	1.27.16 (17 Jul 2024)
Show more unmaintained releases				

Amazon EKS

AMAZON

MANAGED-KUBERNETES

SERVICE

Last updated on 27 September 2024



Amazon Elastic Kubernetes Service (Amazon EKS) is a managed service that you can use to run Kubernetes on AWS without needing to install, operate, and maintain your own Kubernetes control plane or nodes. EKS runs upstream Kubernetes and is certified Kubernetes conformant for a predictable experience.

Release	Released	End of Support	Extended Support	Latest
1.31	1 week and 1 day ago (26 Sep 2024)	Ends in 1 year and 1 month (26 Nov 2025)	Ends in 2 years (26 Nov 2026)	1.31-eks-2 (26 Sep 2024)
1.30	4 months and 2 weeks ago (23 May 2024)	Ends in 9 months (23 Jul 2025)	Ends in 1 year and 9 months (23 Jul 2026)	1.30-eks-8 (03 Sep 2024)
1.29	8 months ago (23 Jan 2024)	Ends in 5 months and 2 weeks (23 Mar 2025)	Ends in 1 year and 5 months (23 Mar 2026)	1.29-eks-13 (03 Sep 2024)
1.28	1 year ago (26 Sep 2023)	Ends in 1 month and 3 weeks (26 Nov 2024)	Ends in 1 year and 1 month (26 Nov 2025)	1.28-eks-19 (03 Sep 2024)
1.27	1 year and 4 months ago (24 May 2023)	Ended 2 months and 1 week ago (24 Jul 2024)	Ends in 9 months (24 Jul 2025)	1.27-eks-23 (03 Sep 2024)
1.26	1 year and 5 months ago (11 Apr 2023)	Ended 3 months and 3 weeks ago (11 Jun 2024)	Ends in 8 months (11 Jun 2025)	1.26-eks-24 (03 Sep 2024)

Broadcom Completes Acquisition of VMware

[\[PDF\]](#) [PDF Version](#)

SAN JOSE, Calif., Nov. 22, 2023 / PRNewswire/ -- Broadcom Inc. (NASDAQ: AVGO), a global technology leader that designs, develops, and supplies semiconductor and infrastructure software

omnissa™



MAY 17, 2024

Setting the record straight: EUC to continue to offer Horizon with vSphere and vSAN

BACK TO PRESS RELEASES

KKR To Acquire Broadcom's End-User Computing Division

February 26, 2024

MENLO PARK, Calif.-(BUSINESS WIRE)- KKR today announced the signing of a definitive agreement with Broadcom

Omnissa Horizon combined offerings with vSphere and vSAN will continue post divestiture (14804)

Last Updated: 1/10/2024

Categories: Informational **Total Views:** 8418

omnissa™



APRIL 25, 2024

Introducing Omnissa, the former VMware End-User Computing business

As a marketing leader, one of the most exhilarating and rewarding undertakings is to define and activate a new brand. And it's a rare opportunity to define a brand for an established business with industry-

Information on Horizon 7 Extended Service Branch (ESB) (52845)

Last Updated: 20/8/2024

Categories: Troubleshooting

Total Views: 586

Acquisition

[\[PDF\]](#) PDF Version

SAN JOSE, Calif.

PRNewswire/ --

AVGO), a global

designs, develop

semiconductor a

omnissa

MAY 17, 2024

Setting the

straight: E

continue to

Horizon w

and vSAN

NOTE

After Broadcom's acquisition of VMWare, Broadcom divested the End-User Computing Division (which includes Horizon) to KKR and branded it as Omnissa as part of the restructuring - which is still in process. Omnissa and Broadcom have entered into a reseller agreement enabling EUC to offer the "combined offering" versions of Horizon SaaS and Horizon Term SKUs with vSphere Foundation for VDI. This combined offering will be available in both Named User and Concurrent User license metrics and for 1-, 3-, and 5-year terms. EUC has no plans to increase Horizon list prices beyond normal annual adjustments.

Starting in Q2 2018, Horizon introduced an option of Extended Service Branch (ESB) in addition to the Current Release (CR) branch. ESBs receive three planned periodic maintenance updates – typically 6 months, 9 months and 15 months after the base version release.

General Support

The last date on which you can request support; the end of regular VMware maintenance updates and upgrades, *bug and security fixes*, and technical assistance as per the Support and Subscription Terms and Conditions.

Omnissa,
/Mware
computing

er, one of the most
arding undertakings is
e a new brand. And
y to define a brand for
ess with industry-

Horizon 7
ce Branch

Last Updated: 1/10/2024

Categories: Informational Total Views: 8418

Total Views: 586

ME TRYING TO FIND OUT

IF A PRODUCT IS SUPPORTED



Stop Chasing CVEs

By

Scored
By

Published
As

40k

MITRE

NIST

NVD

CVEs issued
yearly

Aside 1: NIST/NVD/CVE Drama

- NIST scaled back the NVD program in April 2024.
- As of May 20, of all new vulnerabilities since February 93.4 percent remained unanalyzed.
- NIST amended its five-year, \$125 million IT contract with Maryland-based Analygence to include support for clearing the NVD backlog.
- As of September 21, 2024, 72.4% of CVEs (18,358 CVEs) in the NVD have yet to be analyzed (compared to 93.4% as of May 19, 2024).

NVD Program Announcement

UPDATED - April, 25th 2024

NIST turns to IT consultants to clear National Vulnerability Database backlog

Aims to get CVE logjam cleared by
the end of FY 24

 [Brandon Vigliarolo](#)

Mon 3 Jun 2024 //
21:46 UTC

September 30, 2024

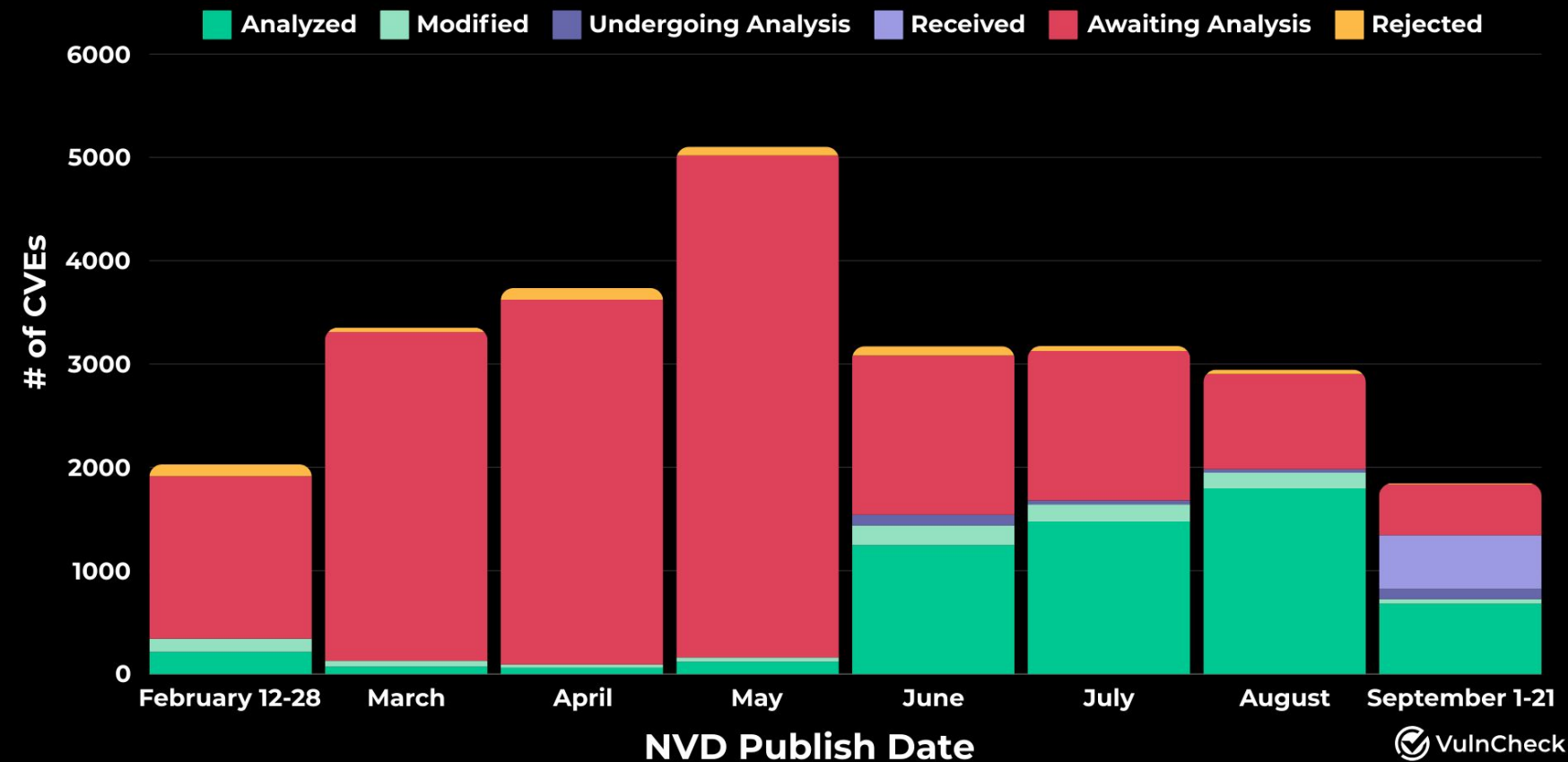
Danger is Still Lurking in the NVD Backlog



Patrick Garrity
[in/patrickmgarrity/](#)

https://www.theregister.com/2024/10/02/cve_pileup_nvd_missed_deadline/

New CVEs in NIST NVD by Status



Aside 2: The CVE System is broken

- [NVD makes up vulnerability severity levels](#)
- [CVE-2020-19909 is everything that is wrong with CVEs](#)
- [NVD damage continued | daniel.haxx.se](#)
- [CVEMITRECVSSNVDCNAOSS WTF - \(Talk\)](#)
- Resume-chasing CVEs

Vulnerability Scanners do not get this nuance.

Stop Chasing CVEs

1/ CVEs are too Late

CVE-2024-6468

Hashicorp Vault vulnerable to Improper Check or Handling of Exceptional Conditions

High severity


GitHub Reviewed

Published on Jul 12 to the GitHub Advisory Database • Updated last month

Vulnerability details

Dependabot alerts 0

Package

 github.com/hashicorp/vault (Go)

Affected versions

>= 1.16.0-rc1, < 1.16.3

>= 1.17.0-rc1, < 1.17.2

>= 1.10.0, < 1.15.12

Patched versions

1.16.3

1.17.2

1.15.12

CVE-2024-6468

Hashicorp Vault vulnerable to Improper Check or Handling of Exceptional Conditions

High severity

GitHub Reviewed

Published on Jul 12 to the GitHub Advisory Database • Updated last month

Vulnerability details

Dependabot alerts 0

Package

 github.com/hashicorp/vault (Go)

Affected versions

$\geq 1.16.0\text{-rc1}$, $< 1.16.3$

$\geq 1.17.0\text{-rc1}$, $< 1.17.2$

$\geq 1.10.0$, $< 1.15.12$

Patched versions

1.  enterprise-only

1.17.2

1.15.12

2/ Fixing a CVE might be impossible

Python

LANG

 Last updated on 03 October 2024 



Python is an interpreted, high-level, general-purpose programming language.

Release	Released	Active Support	Security Support	Latest
3.12	1 year ago (02 Oct 2023)	Ends in 6 months (02 Apr 2025)	Ends in 4 years (31 Oct 2028)	3.12.7 (01 Oct 2024)
3.11	1 year and 11 months ago (24 Oct 2022)	Ended 6 months ago (01 Apr 2024)	Ends in 3 years (31 Oct 2027)	3.11.10 (07 Sep 2024)
3.10	3 years ago (04 Oct 2021)	Ended 1 year and 6 months ago (05 Apr 2023)	Ends in 2 years (31 Oct 2026)	3.10.15 (07 Sep 2024)
3.9	4 years ago (05 Oct 2020)	Ended 2 years and 4 months ago (17 May 2022)	Ends in 1 year (31 Oct 2025)	3.9.20 (06 Sep 2024)
3.8	4 years and 11 months ago (14 Oct 2019)	Ended 3 years and 5 months ago (03 May 2021)	Ends in 3 weeks and 6 days (31 Oct 2024)	3.8.20 (06 Sep 2024)

endoflife.date/python

Python

LANG

Last updated on 03 October 2024



Python is an interpreted, high-level, general-purpose programming language.

Release	Released	Active Support	Security Support	Latest
3.12	1 year ago (02 Oct 2023)	Ends in 6 months (02 Apr 2025)	Ends in 4 years (31 Oct 2028)	3.12.7 (01 Oct 2024)
3.11	1 year and 11 months ago (24 Oct 2022)	Ended 6 months ago (01 Apr 2024)	Ends in 3 years (31 Oct 2027)	3.11.10 (07 Sep 2024)
3.10	3 years ago (04 Oct 2021)	Ended 1 year and 6 months ago (05 Apr 2023)	Ends in 2 years (31 Oct 2026)	3.10.15 (07 Sep 2024)
3.9	4 years ago (05 Oct 2020)	Ended 2 years and 4 months ago (17 May 2022)	Ends in 1 year (31 Oct 2025)	3.9.20 (06 Sep 2024)
3.8	4 years and 11 months ago (14 Oct 2019)	Ended 3 years and 5 months ago (03 May 2021)	Ends in 3 weeks and 6 days (31 Oct 2024)	3.8.20 (06 Sep 2024)

endoflife.date/python

CentOS

DISCONTINUED

LINUX-DISTRIBUTION

OS



Last updated on 15 August 2024



[CentOS Linux](#) was a Linux distribution that provided a free, enterprise-class, community-supported computing platform functionally compatible with [Red Hat Enterprise Linux \(RHEL\)](#).

Release	Released	Active Support	Security Support	Latest
8	5 years ago (24 Sep 2019)	Ended 2 years and 9 months ago (31 Dec 2021)	Ended 2 years and 9 months ago (31 Dec 2021)	8 (2111)
7	10 years ago (07 Jul 2014)	Ended 4 years ago (06 Aug 2020)	Ended 3 months ago (30 Jun 2024)	7 (2009)
6	13 years ago (10 Jul 2011)	Ended 7 years ago (10 May 2017)	Ended 3 years and 10 months ago (30 Nov 2020)	6.10
5	17 years ago (12 Apr 2007)	Ended 10 years ago (31 Jan 2014)	Ended 7 years ago (31 Mar 2017)	5.11

ALPINE 3.18

1.13.5

ARCH

1.17

NIX PKGS 24.05

1.16.2

DOCKERHUB

1.15

CE

BITNAMI

1.17

GENTOO

1.15

CHOCOLATEY

1.17

VAULT-E

1.17

OPENBAO

???

VAULT

1.15

CHAINGUARD

VAULT-GH

1.17

CE

ENTERPRISE

1.15

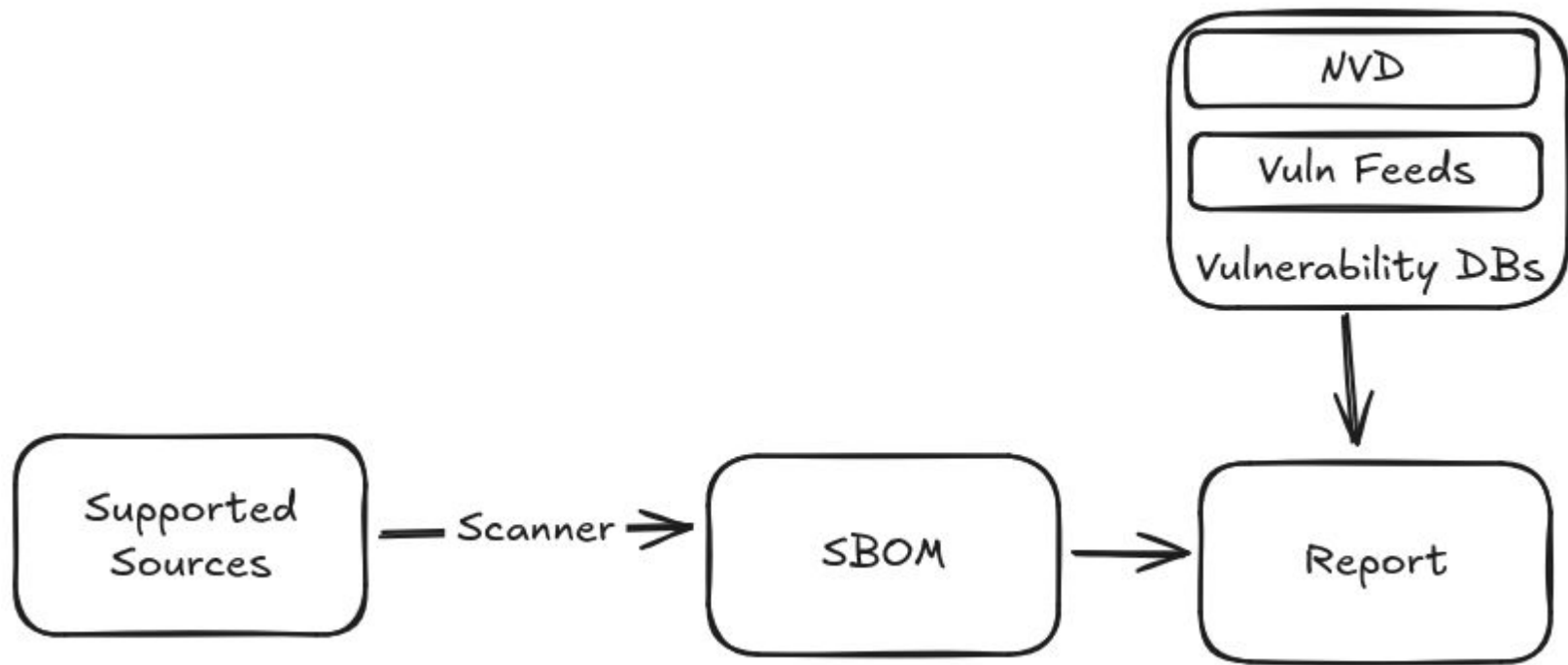
Distro

Container

OSS?

Backporting fixes on your own is harder than it seems.

**4/ Detections can
be misleading.**



A rough representation of how Vulnerability Scanners work.

Your SBOM can lie to you

python:3-slim ❌

```
syft -q packages library/python:3-slim|grep python
pip ..... 22.2.2 ..... python
setuptools ..... 63.2.0 ..... python
wheel ..... 0.37.1 ..... python
```

python:3-alpine ❌

```
syft -q packages library/python:3-alpine|grep python
.python-rundeps ..... 20220907.224335 ..... apk
pip ..... 22.2.2 ..... python
setuptools ..... 63.2.0 ..... python
wheel ..... 0.37.1 ..... python
```

**5/ Regular Updates
are Key**

I'VE FINALLY FOUND
IT... AFTER 15 YEARS



THE SCROLL OF
TRUTH!



Run a
supported
release



NYEH!!



Always run a supported release

Upgrade Safely

- ❑ Have Better Tests
- ❑ Run a minimal distro
- ❑ Use distroless containers

Always run a supported release

Upgrade Safely

- ❑ Have Better Tests
- ❑ Run a minimal/rolling distro
- ❑ Use distroless containers

Regularly

- ❑ Track your Inventory
- ❑ Track your Support Cycles
- ❑ Risk-rank your inventory
- ❑ Understand your Upgrade Paths.

Supply Chain Security is moving fast

- SBOM ecosystem is growing fast.
- NIST/PCI/CIS/... Guidelines are evolving towards this reality.
- Build a Inventory, but double check it.
- Run your scanners, but don't believe them on everything.
- Don't forget cloud versioned services (RDS/EKS/...)

Reach Out



`captnemo.in`