Is This the End of CentOS?

Linux Options for Production Service Providers

Speakers

Sherwin Crown

Senior Member of Technical Staff

MS Computer Science - Cybersecurity / Forensics

Active with Linux since 2001

Mark Lindsey

Senior Member of Technical Staff

MS Computer Science - Mobile / Real Time Networking

Active with Linux since 1991

ECG Makes The Network Work.

RFI, RFP
Selecting software

Configure software
Remediate integration

Acceptance Testing
Compliance Certification

Training & Operations
Voice & Data Networks

BT

windstream®

COX®

Vonage®

bluip™

Deutsche Telekom

AVAYA

Bell

metaswitch

DEPARTMENT OF JUSTICE
QUI PRO DOMINA JUSTITIA SEQUITUR

ECG

What's the "Big Announcement?"

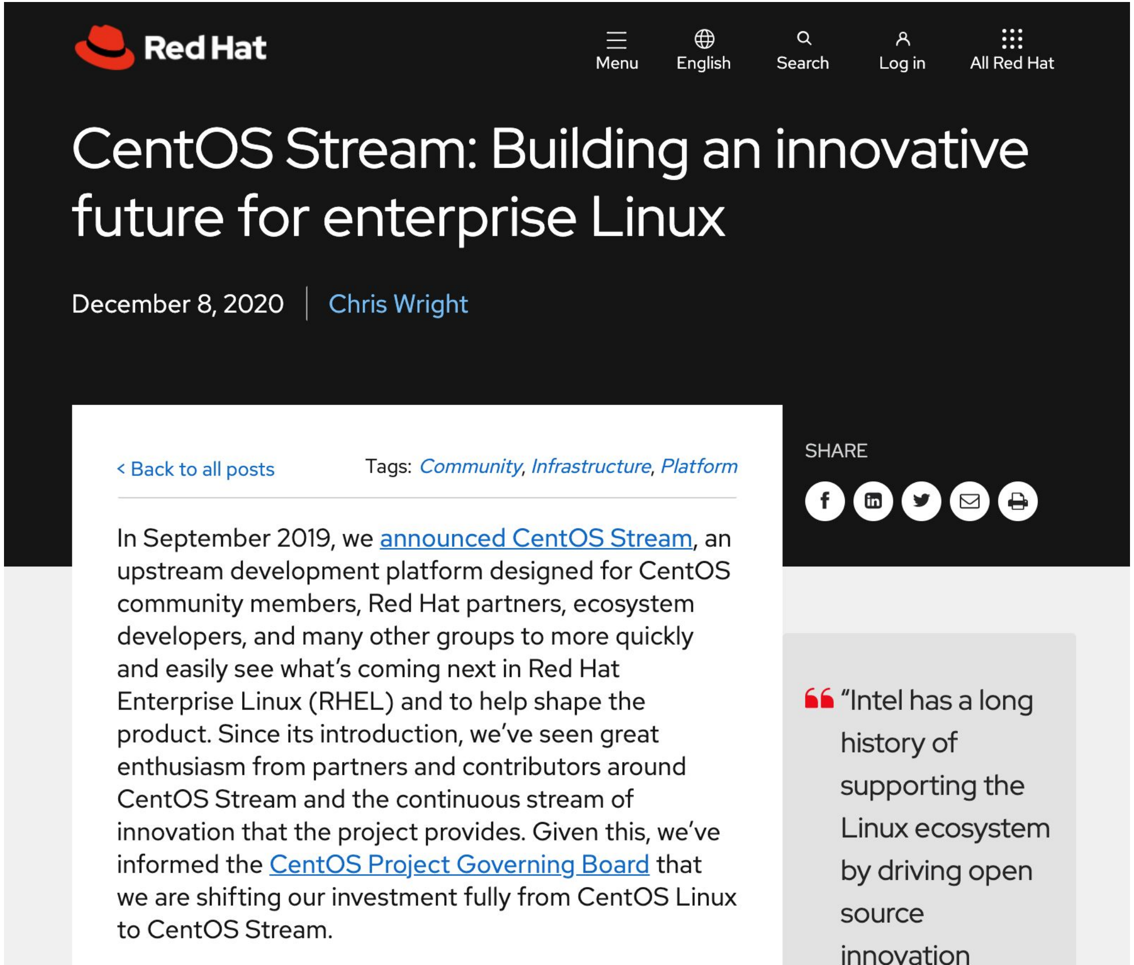
CentOS Linux to be replaced with CentOS Stream

December 8, 2020:

Red Hat (IBM Company) announced the end of CentOS Linux…

…but continued support for CentOS Stream

"CentOS Stream now sits between the Fedora Project's operating system innovation and RHEL's production stability."



CentOS Stream: Building an innovative future for enterprise Linux

December 8, 2020 | Chris Wright

< Back to all posts   Tags: *Community*, *Infrastructure*, *Platform*

In September 2019, we announced CentOS Stream, an upstream development platform designed for CentOS community members, Red Hat partners, ecosystem developers, and many other groups to more quickly and easily see what's coming next in Red Hat Enterprise Linux (RHEL) and to help shape the product. Since its introduction, we've seen great enthusiasm from partners and contributors around CentOS Stream and the continuous stream of innovation that the project provides. Given this, we've informed the CentOS Project Governing Board that we are shifting our investment fully from CentOS Linux to CentOS Stream.

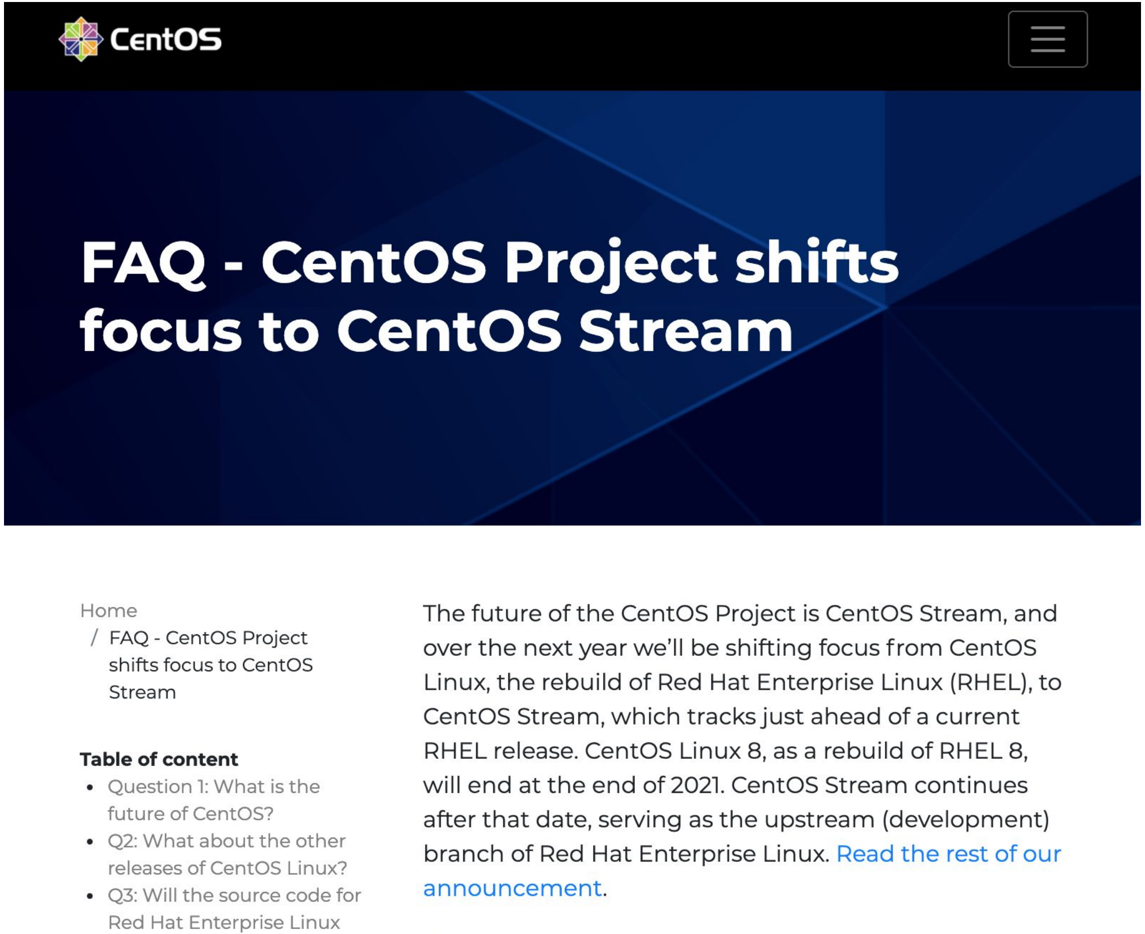
"Intel has a long history of supporting the Linux ecosystem by driving open source innovation

CentOS Announces the change

CentOS organization also announced the end of CentOS Linux

CentOS 8 will receive updates until end of 2021

CentOS 7 will receive updates through 2024



CentOS

FAQ - CentOS Project shifts focus to CentOS Stream

Home / FAQ - CentOS Project shifts focus to CentOS Stream

Table of content

The future of the CentOS Project is CentOS Stream, and over the next year we'll be shifting focus from CentOS Linux, the rebuild of Red Hat Enterprise Linux (RHEL), to CentOS Stream, which tracks just ahead of a current RHEL release. CentOS Linux 8, as a rebuild of RHEL 8, will end at the end of 2021. CentOS Stream continues after that date, serving as the upstream (development) branch of Red Hat Enterprise Linux. Read the rest of our announcement.

Upstream / Downstream

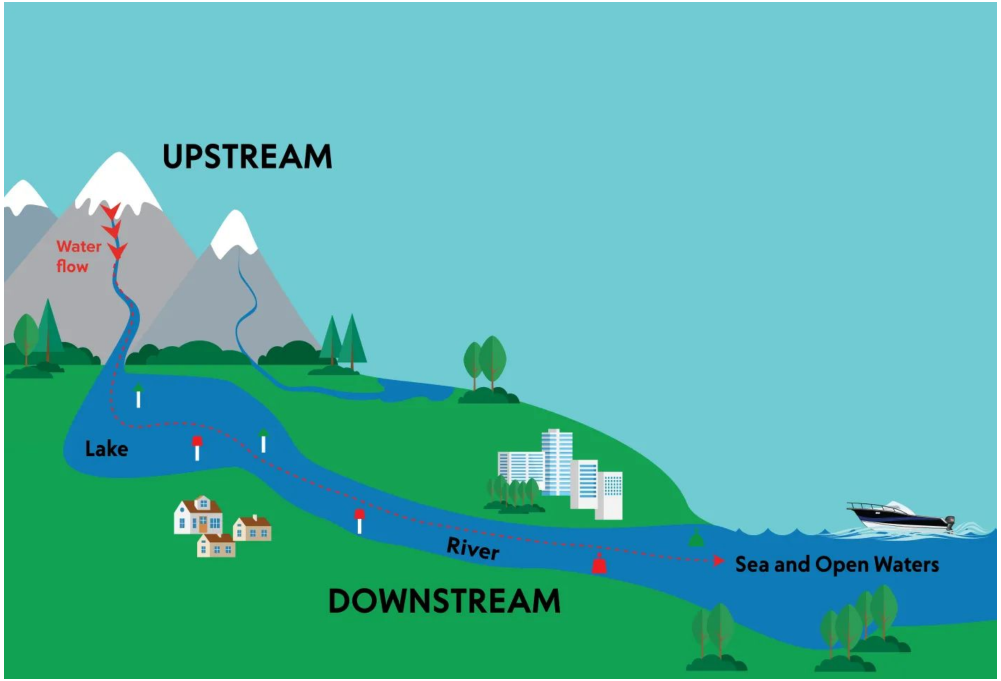


Diagram: thechartroom.co

CentOS Stream "upstream" to RHEL

CentOS Stream is a pre-release, less-tested version - *upstream* to RHEL

CentOS Linux *was downstream* from RHEL - after testing completed

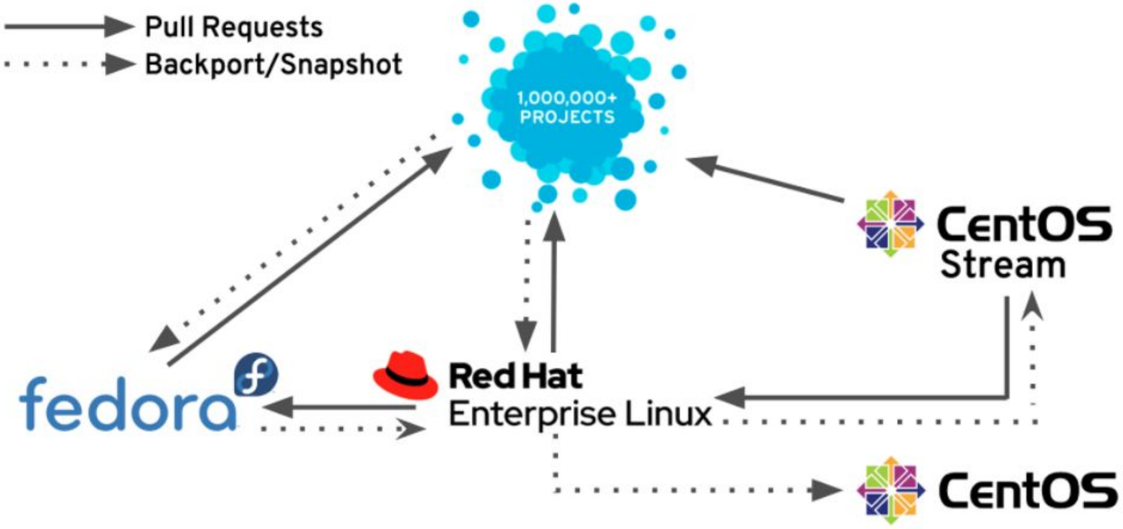
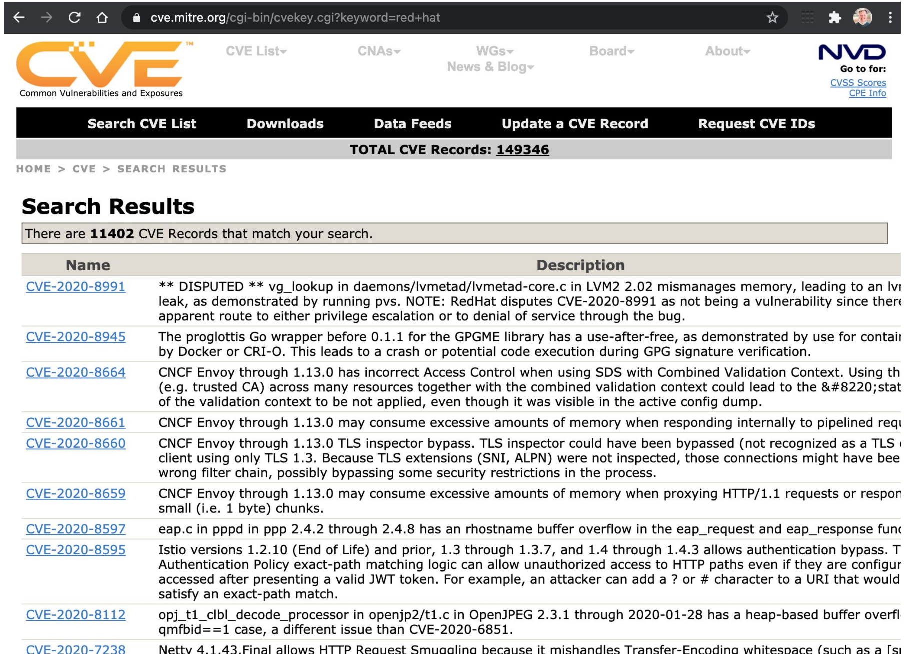


Diagram: The Linux Cluster

What are "updates" and why do they matter?

Linux Updates: Critical for Security

- Linux releases like "CentOS 7.1" or "Red Hat Enterprise Linux 8.2" have a fixed set of features
- Routine software updates largely resolve security issues and substantial software defects
- Security issues are sometimes called CVEs because of "Common Vulnerabilities and Exposures"
- Funded by US Government (DHS CISA)



TOTAL CVE Records: 149346

HOME > CVE > SEARCH RESULTS

Search Results

There are **11402** CVE Records that match your search.

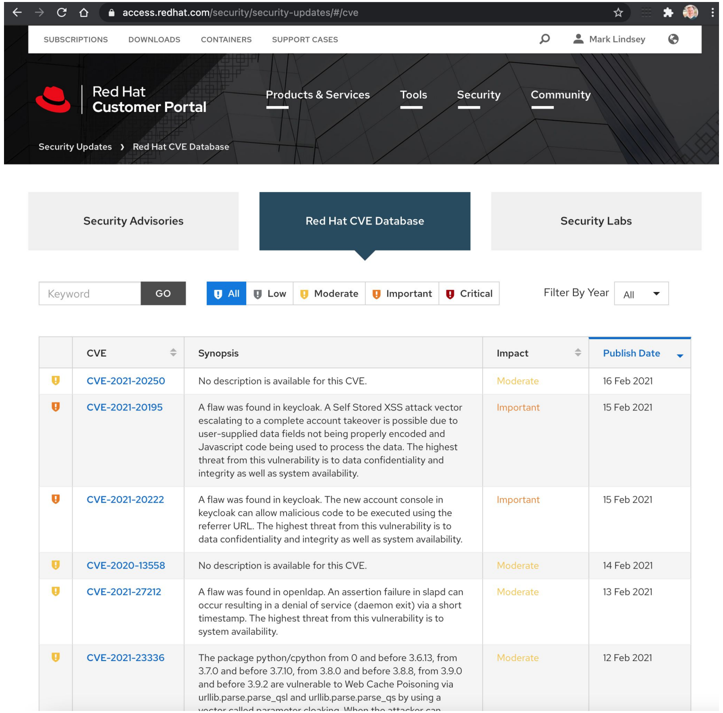
Name	Description
CVE-2020-8991	** DISPUTED ** vg_lookup in daemons/lvmetad/lvmetad-core.c in LVM2 2.02 mismanages memory, leading to an lv leak, as demonstrated by running pvs. NOTE: RedHat disputes CVE-2020-8991 as not being a vulnerability since ther apparent route to either privilege escalation or to denial of service through the bug.
CVE-2020-8945	The proglottis Go wrapper before 0.1.1 for the GPGME library has a use-after-free, as demonstrated by use for contai by Docker or CRI-O. This leads to a crash or potential code execution during GPG signature verification.
CVE-2020-8664	CNCF Envoy through 1.13.0 has incorrect Access Control when using SDS with Combined Validation Context. Using th (e.g. trusted CA) across many resources together with the combined validation context could lead to the &#8220;stat of the validation context to be not applied, even though it was visible in the active config dump.
CVE-2020-8661	CNCF Envoy through 1.13.0 may consume excessive amounts of memory when responding internally to pipelined requ
CVE-2020-8660	CNCF Envoy through 1.13.0 TLS inspector bypass. TLS inspector could have been bypassed (not recognized as a TLS client using only TLS 1.3. Because TLS extensions (SNI, ALPN) were not inspected, those connections might have bee wrong filter chain, possibly bypassing some security restrictions in the process.
CVE-2020-8659	CNCF Envoy through 1.13.0 may consume excessive amounts of memory when proxying HTTP/1.1 requests or respon small (i.e. 1 byte) chunks.
CVE-2020-8597	eap.c in pppd in ppp 2.4.2 through 2.4.8 has an rhostname buffer overflow in the eap_request and eap_response fun
CVE-2020-8595	Istio versions 1.2.10 (End of Life) and prior, 1.3 through 1.3.7, and 1.4 through 1.4.3 allows authentication bypass. T Authentication Policy exact-path matching logic can allow unauthorized access to HTTP paths even if they are configur accessed after presenting a valid JWT token. For example, an attacker can add a ? or # character to a URI that would satisfy an exact-path match.
CVE-2020-8112	opj_t1_clbl_decode_processor in openjp2/t1.c in OpenJPEG 2.3.1 through 2020-01-28 has a heap-based buffer overfl qmfbid==1 case, a different issue than CVE-2020-6851.
CVE-2020-7238	Netty 4.1.43.Final allows HTTP Request Smuggling because it mishandles Transfer-Encoding whitespace (such as a [s

Vulnerabilities are patched to produce updates

Red Hat tracks the vulnerabilities and integrates in patches.

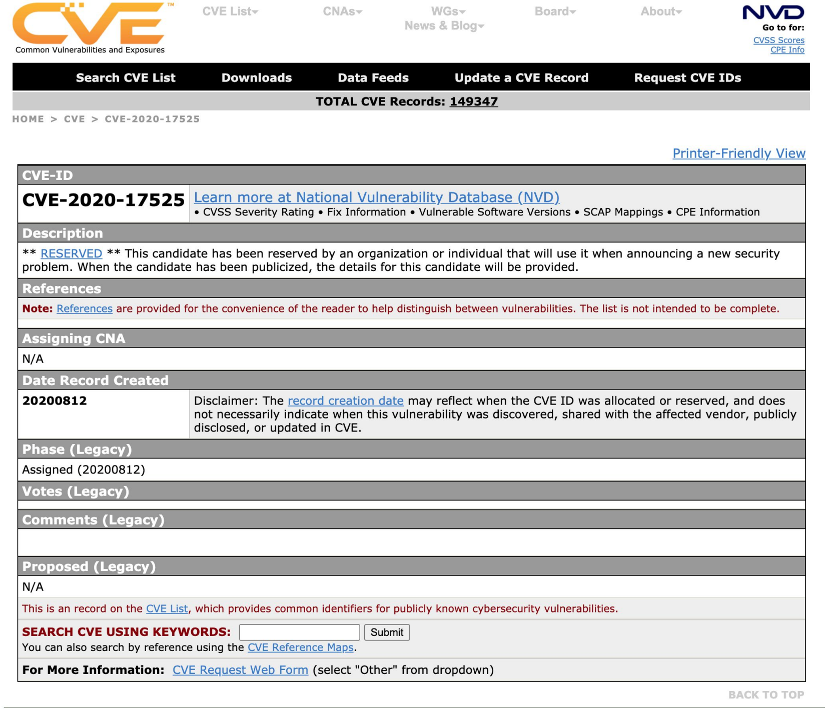
Red Hat calls these "errata"

Subscribers get access to the errata and can easily update their platforms.



	CVE	Synopsis	Impact	Publish Date
!	CVE-2021-20250	No description is available for this CVE.	Moderate	16 Feb 2021
!	CVE-2021-20195	A flaw was found in keycloak. A Self Stored XSS attack vector escalating to a complete account takeover is possible due to user-supplied data fields not being properly encoded and Javascript code being used to process the data. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	Important	15 Feb 2021
!	CVE-2021-20222	A flaw was found in keycloak. The new account console in keycloak can allow malicious code to be executed using the referrer URL. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	Important	15 Feb 2021
!	CVE-2020-13558	No description is available for this CVE.	Moderate	14 Feb 2021
!	CVE-2021-27212	A flaw was found in openldap. An assertion failure in slapd can occur resulting in a denial of service (daemon exit) via a short timestamp. The highest threat from this vulnerability is to system availability.	Moderate	13 Feb 2021
!	CVE-2021-23336	The package python/cpython from 0 and before 3.6.13, from 3.7.0 and before 3.7.10, from 3.8.0 and before 3.8.8, from 3.9.0 and before 3.9.2 are vulnerable to Web Cache Poisoning via urllib.parse.parse_qsl and urllib.parse.parse_qs by using a vector called parameter cloaking. When the attacker can	Moderate	12 Feb 2021

E.g. Bug discovered Aug 12, fix released Feb 15



TOTAL CVE Records: 149347

HOME > CVE > CVE-2020-17525

Printer-Friendly View

CVE-ID

CVE-2020-17525 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

Assigning CNA

N/A

Date Record Created

20200812 Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20200812)

Votes (Legacy)

Comments (Legacy)

Proposed (Legacy)

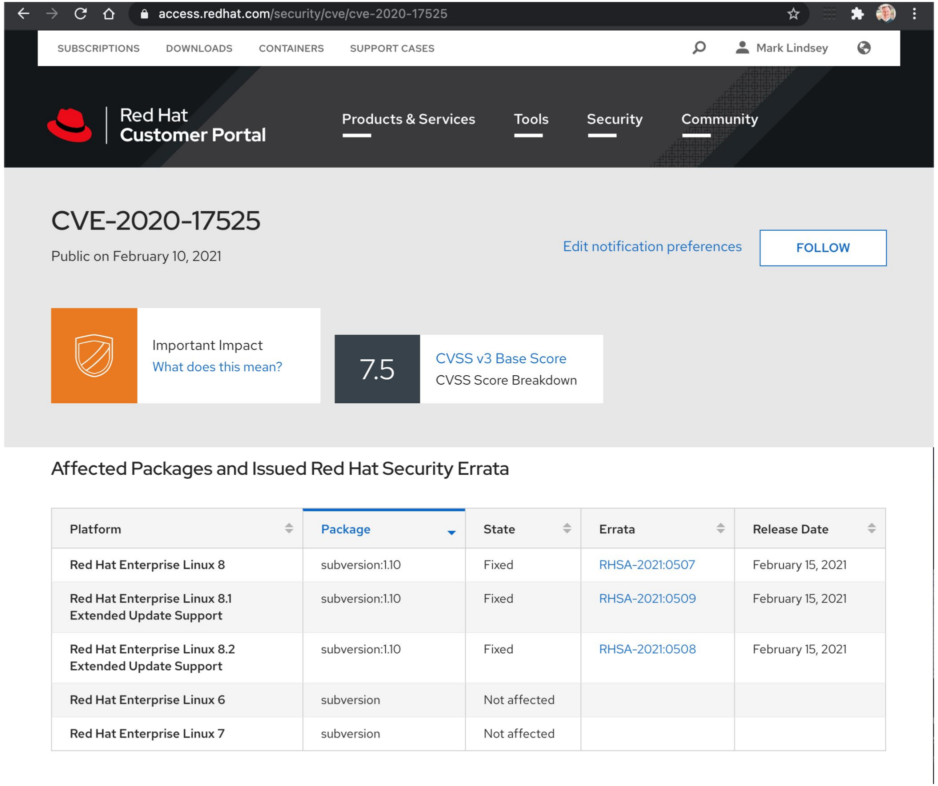
N/A

This is an record on the CVE List, which provides common identifiers for publicly known cybersecurity vulnerabilities.

SEARCH CVE USING KEYWORDS: Submit
You can also search by reference using the CVE Reference Maps.

For More Information: CVE Request Web Form (select "Other" from dropdown)

BACK TO TOP



CVE-2020-17525

Public on February 10, 2021

Edit notification preferences FOLLOW

Important Impact
What does this mean?

7.5 CVSS v3 Base Score
CVSS Score Breakdown

Affected Packages and Issued Red Hat Security Errata

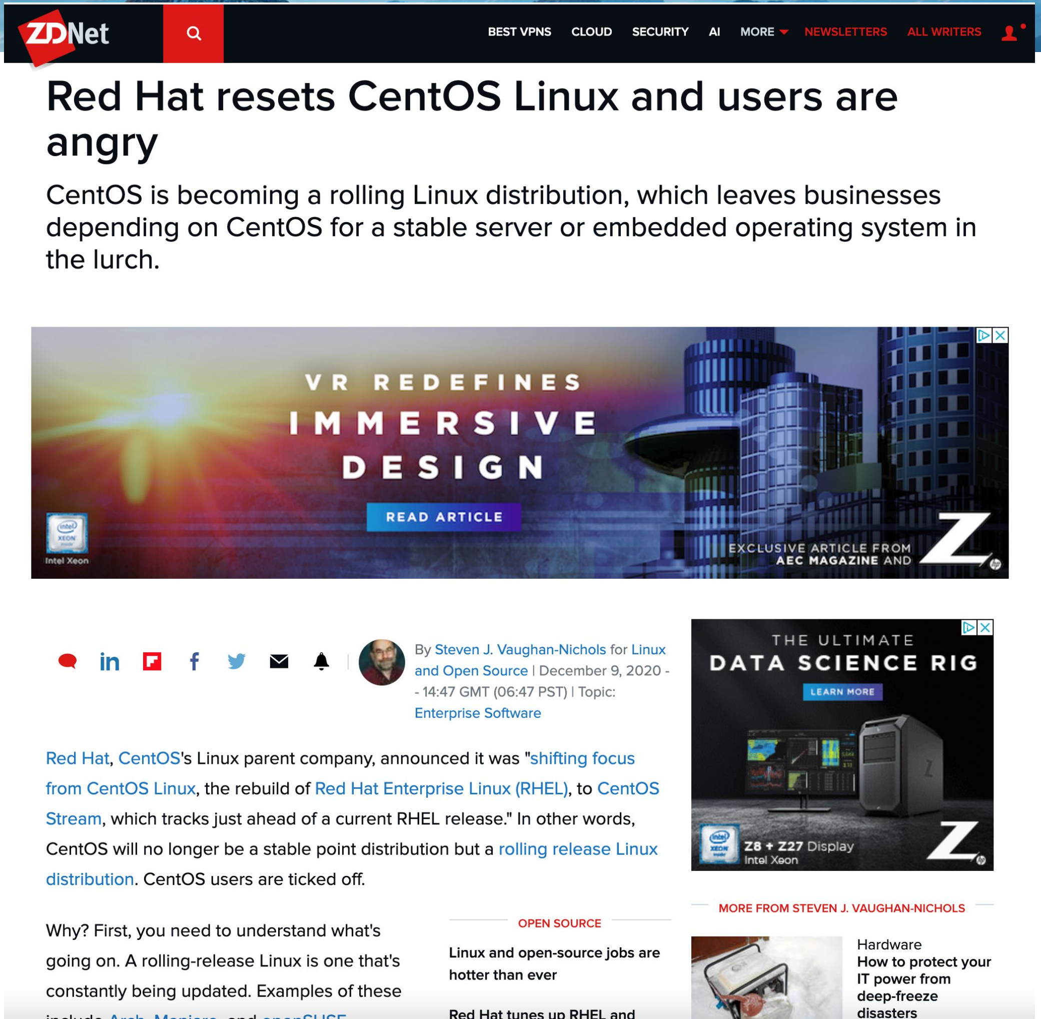
Platform	Package	State	Errata	Release Date
Red Hat Enterprise Linux 8	subversion:1.10	Fixed	RHSA-2021:0507	February 15, 2021
Red Hat Enterprise Linux 8.1 Extended Update Support	subversion:1.10	Fixed	RHSA-2021:0509	February 15, 2021
Red Hat Enterprise Linux 8.2 Extended Update Support	subversion:1.10	Fixed	RHSA-2021:0508	February 15, 2021
Red Hat Enterprise Linux 6	subversion	Not affected		
Red Hat Enterprise Linux 7	subversion	Not affected		

What is the industry response?

"Users are Angry" - Steven Vaughan-Nichols, ZDNet

"In any case, it's very clear that Red Hat doesn't see CentOS Stream as a production server. As a server for RHEL customers to use to see what the next version of RHEL will bring to them, yes, but for day-to-day work? No"

"Red Hat will continue to support CentOS 7 and produce it through the remainder of the RHEL 7 life cycle. ...CentOS 7, you'll see support through June 30, 2024. ..may also offer extended life cycle support for RHEL and CentOS 7"



Red Hat resets CentOS Linux and users are angry

CentOS is becoming a rolling Linux distribution, which leaves businesses depending on CentOS for a stable server or embedded operating system in the lurch.

By Steven J. Vaughan-Nichols for Linux and Open Source | December 9, 2020 -- 14:47 GMT (06:47 PST) | Topic: Enterprise Software

Red Hat, CentOS's Linux parent company, announced it was "shifting focus from CentOS Linux, the rebuild of Red Hat Enterprise Linux (RHEL), to CentOS Stream, which tracks just ahead of a current RHEL release." In other words, CentOS will no longer be a stable point distribution but a rolling release Linux distribution. CentOS users are ticked off.

Why? First, you need to understand what's going on. A rolling-release Linux is one that's constantly being updated. Examples of these include Arch, Manjaro, and openSUSE

OPEN SOURCE

Linux and open-source jobs are hotter than ever

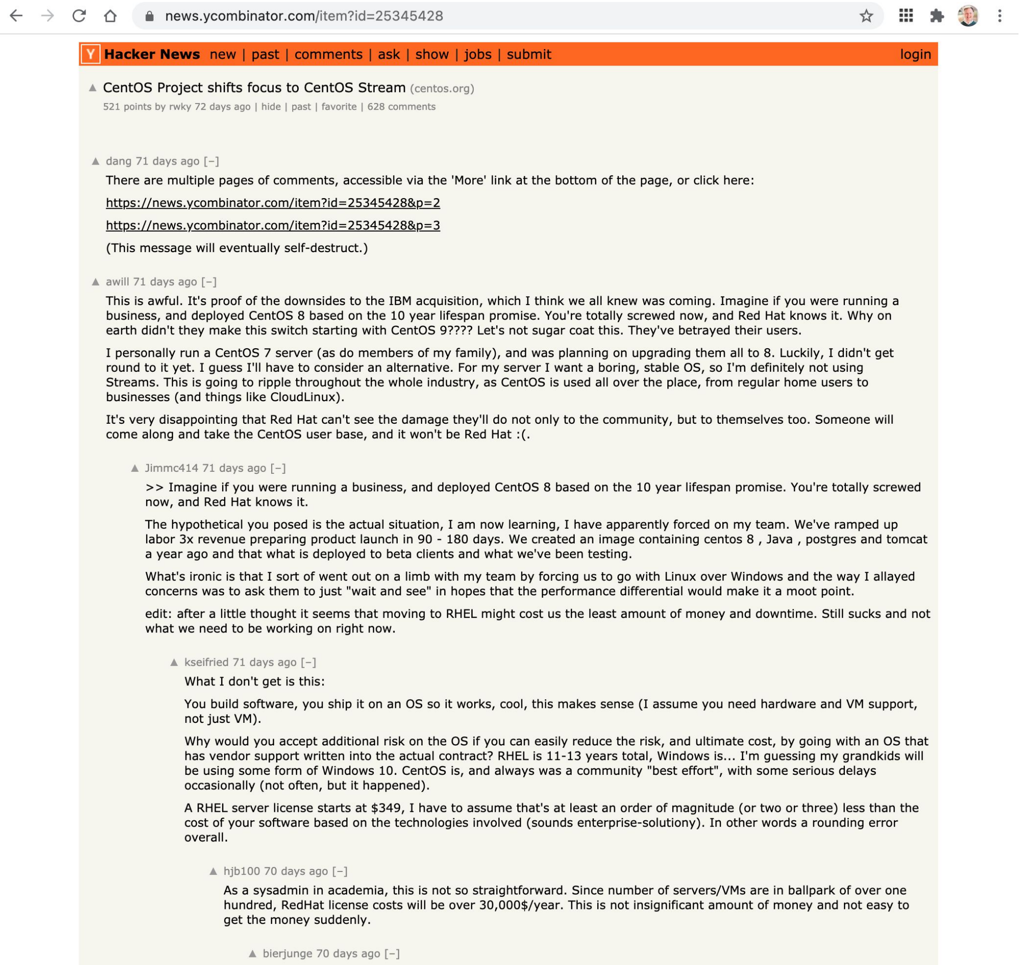
Red Hat tunes up RHEL and

MORE FROM STEVEN J. VAUGHAN-NICHOLS

Hardware
How to protect your IT power from deep-freeze disasters

"They've betrayed us." - Hacker News

"Imagine if you were running a business, and deployed CentOS 8 based on the 10-year lifespan promise. You're totally screwed now, and Red Hat knows it. Why on earth didn't they make this switch starting with CentOS 9???? Let's not sugar coat this. They've betrayed us."


news.ycombinator.com/item?id=25345428
Y Hacker News new | past | comments | ask | show | jobs | submit
login

▲ CentOS Project shifts focus to CentOS Stream (centos.org)

521 points by rwky 72 days ago | hide | past | favorite | 628 comments

▲ dang 71 days ago [–]

There are multiple pages of comments, accessible via the 'More' link at the bottom of the page, or click here:

https://news.ycombinator.com/item?id=25345428&p=2

https://news.ycombinator.com/item?id=25345428&p=3

(This message will eventually self-destruct.)

▲ awill 71 days ago [–]

This is awful. It's proof of the downsides to the IBM acquisition, which I think we all knew was coming. Imagine if you were running a business, and deployed CentOS 8 based on the 10 year lifespan promise. You're totally screwed now, and Red Hat knows it. Why on earth didn't they make this switch starting with CentOS 9???? Let's not sugar coat this. They've betrayed their users.

I personally run a CentOS 7 server (as do members of my family), and was planning on upgrading them all to 8. Luckily, I didn't get round to it yet. I guess I'll have to consider an alternative. For my server I want a boring, stable OS, so I'm definitely not using Streams. This is going to ripple throughout the whole industry, as CentOS is used all over the place, from regular home users to businesses (and things like CloudLinux).

It's very disappointing that Red Hat can't see the damage they'll do not only to the community, but to themselves too. Someone will come along and take the CentOS user base, and it won't be Red Hat :(.

▲ Jimmc414 71 days ago [–]

>> Imagine if you were running a business, and deployed CentOS 8 based on the 10 year lifespan promise. You're totally screwed now, and Red Hat knows it.

The hypothetical you posed is the actual situation, I am now learning, I have apparently forced on my team. We've ramped up labor 3x revenue preparing product launch in 90 - 180 days. We created an image containing centos 8 , Java , postgres and tomcat a year ago and that what is deployed to beta clients and what we've been testing.

What's ironic is that I sort of went out on a limb with my team by forcing us to go with Linux over Windows and the way I allayed concerns was to ask them to just "wait and see" in hopes that the performance differential would make it a moot point.

edit: after a little thought it seems that moving to RHEL might cost us the least amount of money and downtime. Still sucks and not what we need to be working on right now.

▲ kseifried 71 days ago [–]

What I don't get is this:

You build software, you ship it on an OS so it works, cool, this makes sense (I assume you need hardware and VM support, not just VM).

Why would you accept additional risk on the OS if you can easily reduce the risk, and ultimate cost, by going with an OS that has vendor support written into the actual contract? RHEL is 11-13 years total, Windows is... I'm guessing my grandkids will be using some form of Windows 10. CentOS is, and always was a community "best effort", with some serious delays occasionally (not often, but it happened).

A RHEL server license starts at $349, I have to assume that's at least an order of magnitude (or two or three) less than the cost of your software based on the technologies involved (sounds enterprise-solutiony). In other words a rounding error overall.

▲ hjb100 70 days ago [–]

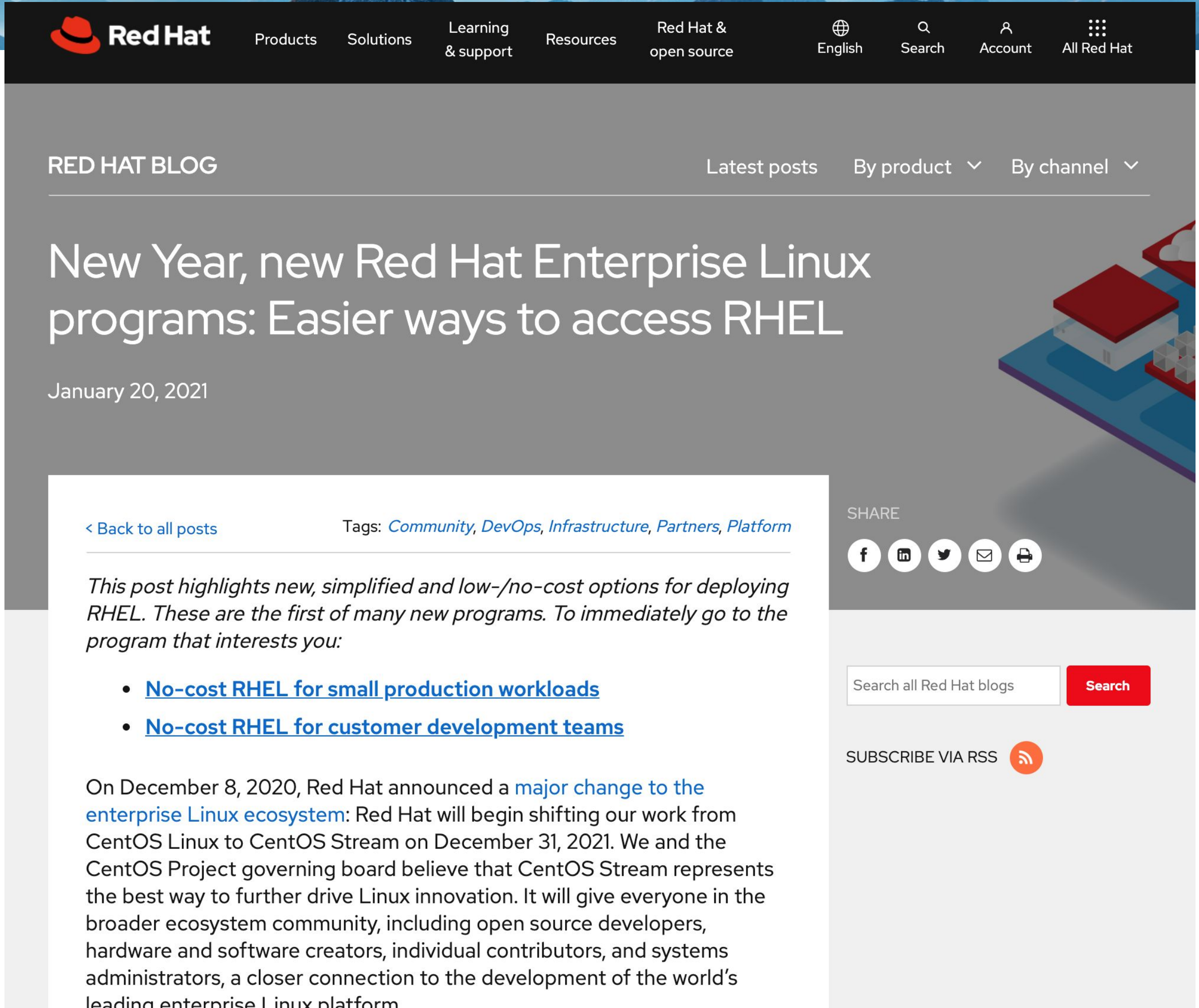
As a sysadmin in academia, this is not so straightforward. Since number of servers/VMs are in ballpark of over one hundred, RedHat license costs will be over 30,000$/year. This is not insignificant amount of money and not easy to get the money suddenly.

▲ bierjunge 70 days ago [–]

What options do operators have?

RHEL free for up to 16 production servers

"We’re addressing this by expanding the terms of the Red Hat Developer program so that the *Individual Developer subscription* for RHEL can be used in production for up to 16 systems. That’s exactly what it sounds like: for small production use cases, this is no-cost, self-supported RHEL."



New Year, new Red Hat Enterprise Linux programs: Easier ways to access RHEL

January 20, 2021

< Back to all posts

Tags: *Community*, *DevOps*, *Infrastructure*, *Partners*, *Platform*

This post highlights new, simplified and low-/no-cost options for deploying RHEL. These are the first of many new programs. To immediately go to the program that interests you:

- No-cost RHEL for small production workloads
- No-cost RHEL for customer development teams

On December 8, 2020, Red Hat announced a major change to the enterprise Linux ecosystem: Red Hat will begin shifting our work from CentOS Linux to CentOS Stream on December 31, 2021. We and the CentOS Project governing board believe that CentOS Stream represents the best way to further drive Linux innovation. It will give everyone in the broader ecosystem community, including open source developers, hardware and software creators, individual contributors, and systems administrators, a closer connection to the development of the world’s leading enterprise Linux platform

ZDNet lists alternatives

1. CentOS Stream (🐶 🧪)

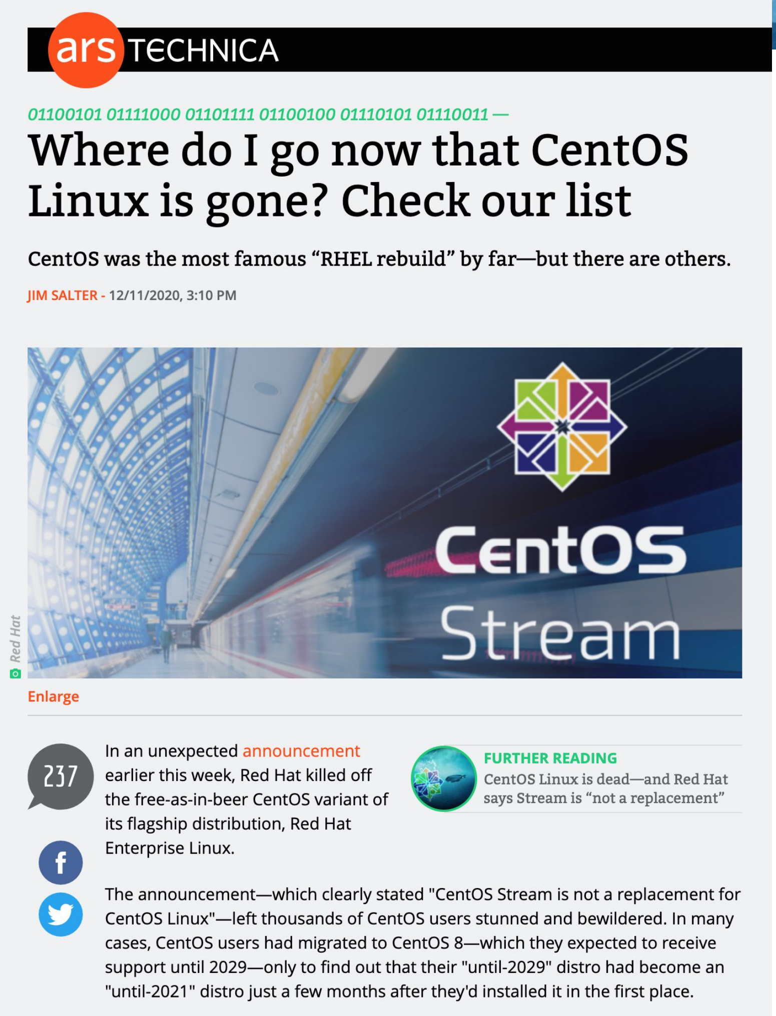
2. Oracle Linux ($ 🏢)

3. Cloud Linux ($ 👻)

4. Springdale Linux (🐶 🏫)

5. Rocky Linux (🐶 👻)

6. HPE ClearOS (🐶 🏢 🧪)



ars TECHNICA

01100101 01111000 01101111 01100100 01110101 01110011 —

Where do I go now that CentOS Linux is gone? Check our list

CentOS was the most famous "RHEL rebuild" by far—but there are others.

JIM SALTER - 12/11/2020, 3:10 PM

Red Hat

Enlarge

237

In an unexpected announcement earlier this week, Red Hat killed off the free-as-in-beer CentOS variant of its flagship distribution, Red Hat Enterprise Linux.

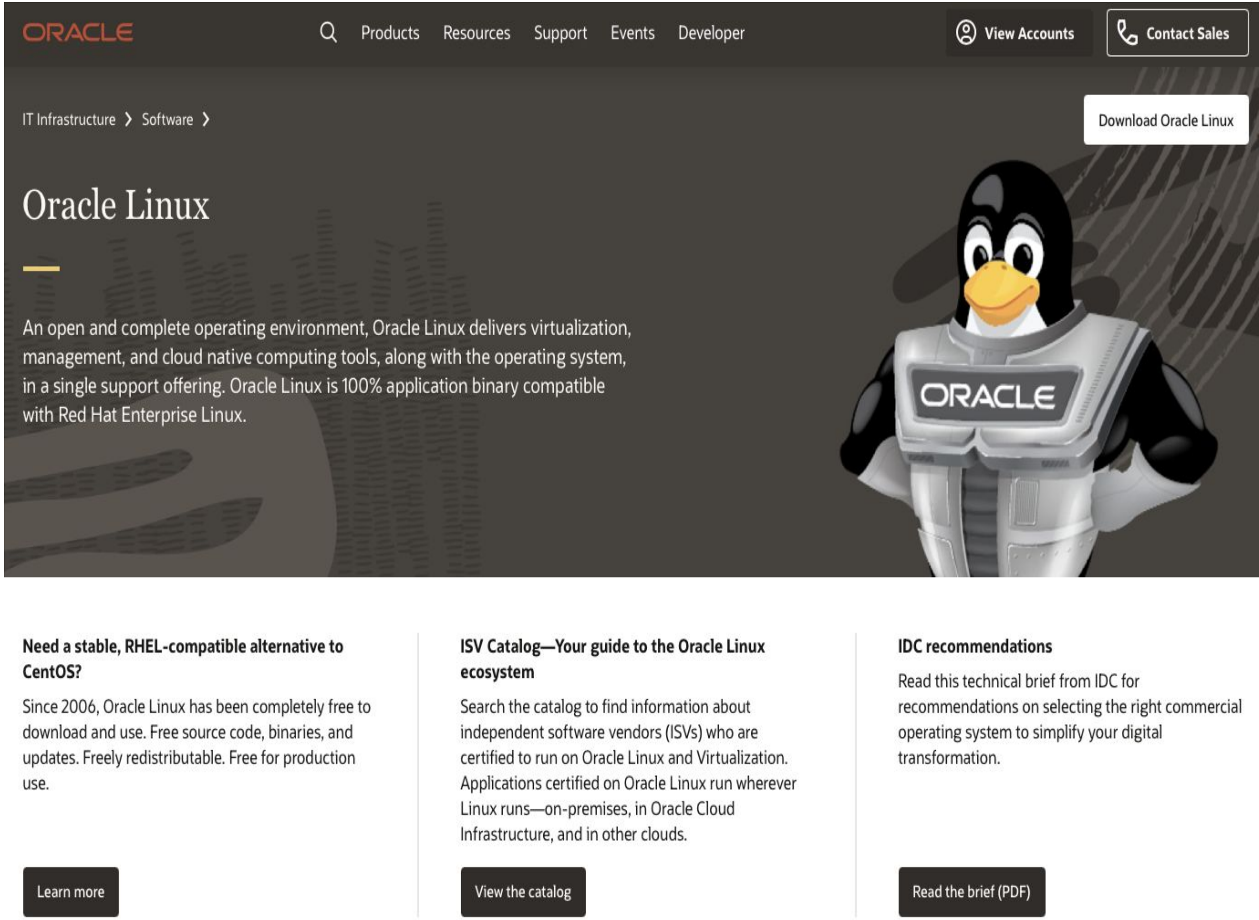
FURTHER READING
CentOS Linux is dead—and Red Hat says Stream is "not a replacement"

The announcement—which clearly stated "CentOS Stream is not a replacement for CentOS Linux"—left thousands of CentOS users stunned and bewildered. In many cases, CentOS users had migrated to CentOS 8—which they expected to receive support until 2029—only to find out that their "until-2029" distro had become an "until-2021" distro just a few months after they'd installed it in the first place.

Oracle Linux free to use with optional support

“We're putting Oracle Linux in your hands by doing two things:

- We've made the Oracle Linux software available free of charge
- We've created a simple script to switch your CentOS systems to Oracle Linux”



Oracle Linux

An open and complete operating environment, Oracle Linux delivers virtualization, management, and cloud native computing tools, along with the operating system, in a single support offering. Oracle Linux is 100% application binary compatible with Red Hat Enterprise Linux.

Need a stable, RHEL-compatible alternative to CentOS?

Since 2006, Oracle Linux has been completely free to download and use. Free source code, binaries, and updates. Freely redistributable. Free for production use.

ISV Catalog—Your guide to the Oracle Linux ecosystem

Search the catalog to find information about independent software vendors (ISVs) who are certified to run on Oracle Linux and Virtualization. Applications certified on Oracle Linux run wherever Linux runs—on-premises, in Oracle Cloud Infrastructure, and in other clouds.

IDC recommendations

Read this technical brief from IDC for recommendations on selecting the right commercial operating system to simplify your digital transformation.

Other top (non-RHEL-based) server distributions

1. Ubuntu
2. Debian
3. openSUSE

What are the key considerations?
(So what?)

End of updates is coming

After 2024, CentOS 7 won't get security updates

- This means a major vulnerability discovered in January 2025 will not be patched
- 3 years is a short lifespan for a Virtual Machine!

After 2021, CentOS 8 won't get updates

Budgeting

- If you were using CentOS, you weren't paying anybody for updates

- You may need to plan to pay a vendor to keep access to updates
  - Red Hat - >= $349 per server (VM) and up
  - Oracle - >= $1200 per physical server

- Easy and proven option: ***Move to RHEL***
  - No substantial migration complexity
  - Red Hat has a deep skill level and can do a great job of support on complex issues (e.g., custom kernel patch to fix a bug in a driver)

Migration / retraining?

- If you're switching to another distribution, the system management can vary substantially

- Especially important if you're using automation tools
  - Ansible
  - Puppet
  - Chef

Continue the Conversation

Mark R Lindsey, mark@ecg.co, +1-229-316-0013
Schedule a chat: https://ecg.co/lindsey/meeting

Sherwin Crown, scrown@ecg.co, +1-229-316-0015

Trevor Wolford, twolford@ecg.co, +1-229-316-0435
Account Manager