Delivery Deadline Radar: 22 Engineering Deadlines and a 30-Minute Check for Each

A quarterly list of regulations, end-of-support dates and platform changes that affect software delivery. Every item has a date, the teams it affects, a check one engineer can run in about thirty minutes and a recommended action.

For: Engineering leaders who want every dated change in one list, with a thirty-minute check for each.

By Subeesh Sivanandan, Founder, Stonetusker Systems · Updated 29 October 2026 · About 17 minutes to read · PDF version

Technical and engineering guidance. Please confirm legal obligations with your own counsel.

The short version

- In force now: Cyber Resilience Act reporting for products sold in the European Union (since 11 September 2026, with an early warning within 24 hours) and the 2026 minimum elements for a software bill of materials (final since late July 2026).[1,2]

- Already past, and easy to miss because nothing failed on the day: Ingress NGINX (March 2026), Yocto Kirkstone (April 2026), the Bitnami catalog change (from 28 August 2025), Node 20 on GitHub runners (23 September 2026), cgroup v1 in Kubernetes 1.35, CDK for Terraform, Debian 11 (31 August 2026), Python 3.10 (1 October 2026) and Kubernetes 1.34 (27 October 2026).
- Coming next: the macOS 14 runner image (2 November 2026), .NET 8 and .NET 9 (10 November 2026) and the Product Liability Directive (products placed on the market after 8 December 2026; transposition by 9 December 2026). Certificate lifetimes, the Artificial Intelligence Act and the full Cyber Resilience Act follow in 2027 and 2028.
- To watch: Cybersecurity Maturity Model Certification Phase 2 (suspended on 13 July 2026, no restart date), GitHub Actions runner pricing and Docker Hub pull limits.
- How to use it: find your archetype, run the thirty-minute check for each item that applies, and put every open item in the roadmap with an owner and a date.

22
Dated changes tracked in this edition

24 hours
To send a Cyber Resilience Act early warning for an exploited vulnerability[1]

100 days
Maximum public certificate life from 15 March 2027[8]

How to use this radar

Pick the rows in the tables below that match your stack and run the thirty-minute check for each. A clean result closes the item until the next edition. Any other result is a dated, scoped piece of work for the roadmap. Each item carries one of four statuses: **in force**, **end of support**, **coming** or **to watch**.

Start from your archetype

What constrains a release depends less on the industry than on what has to be true before it ships. Many companies sit in two archetypes, so please read both rows.

Archetype and typical industries	Check these items first
1. Hardware-bound and safety-critical Embedded and defence, automotive, energy and telecommunications Five-minute checklist	Cyber Resilience Act reporting, Yocto Kirkstone, Product Liability Directive, Cyber Resilience Act in full
2. Regulated data and audit-first Healthcare and medical technology, financial services, public sector, education Five-minute checklist	2026 software bill of materials elements, 100-day certificates, Product Liability Directive, Cybersecurity Maturity Model Certification for defense suppliers
3. Ultra-scale and high availability Ecommerce, travel, gaming and streaming, advertising Five-minute checklist	100-day certificates, Let's Encrypt 64-day certificates, Ingress NGINX, Kubernetes 1.34, Docker Hub limits; note: before the peak-season freeze
4. Artificial intelligence, machine learning and data Model and data platform companies, and products with models inside Five-minute checklist	Artificial Intelligence Act dates, Python 3.10, Bitnami images, Kubernetes 1.34; note: model lineage
5. Developer experience and modernisation Cloud software platforms, security vendors, enterprise internal systems Five-minute checklist	Node 20, macOS 14 runner, .NET 8 and .NET 9, CDK for Terraform, runner pricing, coding assistant baseline

All items at a glance

Date	Change	Status	Mainly affects
28 August 2025	Bitnami catalog change	End of support	Kubernetes and Helm users
December 2025	Kubernetes 1.35 and cgroup v1	End of support	Platform teams
10 December 2025	CDK for Terraform archived	End of support	Infrastructure teams
March 2026	Ingress NGINX retired	End of support	Kubernetes users
April 2026	Yocto Kirkstone end of support	End of support	Embedded Linux teams
30 April to 23 September 2026	Node 20 removed from GitHub runners	End of support	GitHub Actions users
13 July 2026	Cybersecurity Maturity Model Certification Phase 2 suspended	To watch	United States defense supply chain
Late July 2026	2026 software bill of materials elements	In force	Vendors to United States and regulated buyers
31 August 2026	Debian 11 long-term support ends	End of support	Container and Linux platform teams
11 September 2026	Cyber Resilience Act reporting	In force	Products sold in the European Union
1 October 2026	Python 3.10 end of life	End of support	Python services and pipelines

Date	Change	Status	Mainly affects
27 October 2026	Kubernetes 1.34 end of maintenance	End of support	Platform teams
2 November 2026	macOS 14 runner image retired	Coming	GitHub Actions users on macOS
10 November 2026	.NET 8 and .NET 9 end of support	Coming	.NET services and functions
9 December 2026	Product Liability Directive covers software	Coming	Software and device makers selling in the European Union
10 February 2027	Let's Encrypt 64-day default certificates	Coming	Let's Encrypt users
15 March 2027	100-day public certificates	Coming	Every organisation
2 December 2027 and 2 August 2028	European Union Artificial Intelligence Act high-risk obligations	Coming	High-risk artificial intelligence systems
11 December 2027	Cyber Resilience Act in full	Coming	Products sold in the European Union
Ongoing	GitHub runner pricing and Docker Hub limits	To watch	Pipeline owners
Before your next budget cycle	Coding assistant delivery baseline	Practice	Engineering leaders

Rules already in force

Cyber Resilience Act: 24-hour vulnerability reporting

Status	In force since 11 September 2026
Who it affects	Manufacturers of hardware and software products with digital elements sold in the European Union, including products already on the market.
What changes	Actively exploited vulnerabilities and severe incidents must be reported through the Single Reporting Platform: an early warning within 24 hours and a notification within 72 hours.[1] Fines reach 15 million euros or 2.5% of worldwide turnover.[9]
Thirty-minute check	Can someone list every component and version in the firmware or software release that most European customers run, within 15 minutes, from stored records?
Recommended action	Name a reporting owner, arrange access to the platform, and store a software bill of materials for every shipped release.
Further reading	Cyber Resilience Act reporting and Yocto Kirkstone

2026 minimum elements for a software bill of materials

Status	Final since late July 2026
Who it affects	Software and device vendors that sell to United States federal agencies, regulated industries or security-focused enterprise buyers.
What changes	It updates the 2021 baseline.[2] New elements include component hashes, licences, the generating tool, generation context and an author signature.

Thirty-minute check	Open your latest software bill of materials, count the components with a hash and a licence, and check whether it records its generation context.
Recommended action	Produce the record inside the build, with hashes and package identifiers, and sign it.
Further reading	The 2026 minimum elements

Tools and versions past end of support

Teams miss this group most often. Nothing stopped working on the day. The fixes ended, and the risk arrives with the next vulnerability or upgrade.

Ingress NGINX retired

Status	End of support, March 2026
Who it affects	Kubernetes clusters that use the community Ingress NGINX controller, which the Kubernetes committees say covered about half of cloud native environments.[3]
What changes	The project has stopped publishing releases, bug fixes and security updates. Existing installations keep running, which is why the change is easy to miss.
Thirty-minute check	`kubectl get pods --all-namespaces --selector app.kubernetes.io/name=ingress-nginx` on every cluster.
Recommended action	Plan the move to Gateway API, or to a supported controller as a bridge.
Further reading	Ingress NGINX migration plan

Yocto Project 4.0 Kirkstone out of support

Status	End of support, April 2026
Who it affects	Embedded Linux products built on Kirkstone, often through a chip vendor's board support package.
What changes	Point releases and security fixes from the project have ended, so each fix becomes your own backport. Scarthgap is supported until April 2028 and Wrynose until April 2030.[4]
Thirty-minute check	`grep -r --include=layer.conf LAYERSERIES_CORENAMES .` in the build tree of each shipping product.
Recommended action	Decide per product: upgrade, fund extended maintenance for a fixed period, or set an end-of-sale date.
Further reading	Cyber Resilience Act reporting and Yocto Kirkstone

Bitnami catalog change

Status	Changes from 28 August 2025
Who it affects	Teams that run Bitnami container images or Helm charts, often for PostgreSQL, Redis, Kafka and similar services.
What changes	From 28 August 2025 versioned images were archived in the bitnamilegacy repository, which stays at its last update, and their removal from the public catalog was scheduled for 29 September 2025.[5,25] Free images are available on the latest tag only, and maintained versions need a paid subscription.
Thirty-minute check	Search your repositories for `bitnamilegacy` and list running images that contain `bitnami`.

Recommended action	Replace each component in a planned order, then mirror images into your own registry and pin them by digest.
Further reading	Bitnami images: find and replace

Node 20 removed from GitHub Actions runners

Status	Removed from runners, 23 September 2026
Who it affects	Teams that use GitHub Actions, especially with their own JavaScript actions or older action versions.
What changes	Node 20 reached end of life on 30 April 2026. GitHub runners used Node 24 by default from 16 June 2026 with a temporary opt-out, and GitHub removed Node 20 from its runners on 23 September 2026, which also ended the opt-out.[6]
Thirty-minute check	Search your own actions for `using: node20` in `action.yml`, and look for older major versions of common actions in your workflows.
Recommended action	Move custom actions to node24 and update third-party actions to current major versions. With shared workflow templates this is one change instead of many.
Further reading	GitHub changelog

Kubernetes nodes on cgroup v1 fail to start

Status	Since Kubernetes 1.35, December 2025
Who it affects	Clusters whose nodes run older operating system images that still use cgroup v1.

What changes	From Kubernetes 1.35 the kubelet refuses to start on cgroup v1 nodes by default.[7] The issue appears during upgrades as nodes that fail to become ready.
Thirty-minute check	On a node, `stat -fc %T /sys/fs/cgroup/` prints `cgroup2fs` for cgroup v2. Any other result needs attention.
Recommended action	Move node images to cgroup v2 before the upgrade, and rehearse the upgrade on a non-production cluster.
Further reading	Kubernetes enhancement proposal 5573

CDK for Terraform archived

Status	Archived 10 December 2025
Who it affects	Teams that define infrastructure with CDK for Terraform in TypeScript, Python, Go, Java or C#.
What changes	HashiCorp archived the project and ended its maintenance and development.[14] Provider bindings and dependencies will drift over time.
Thirty-minute check	Search your repositories for `cdktf.json`.
Recommended action	Plan a move per stack to Terraform or OpenTofu configuration, or to another infrastructure-as-code tool, before a provider upgrade forces it.
Further reading	env zero: what the change means

Debian 11 bullseye out of long-term support

Status	End of long-term support, 31 August 2026

Who it affects	Container images built on `debian:bullseye` or other bullseye-based images, and servers or devices that run Debian 11.
What changes	The Debian Long Term Support team ended support for Debian 11 on 31 August 2026, and Debian no longer publishes security updates for it. Debian 12 receives long-term support until 30 June 2028.[18]
Thirty-minute check	`grep -rnE 'FROM .*(bullseye|debian:11)' --include='Dockerfile*' .` in your repositories, and `cat /etc/debian_version` on hosts.
Recommended action	Rebuild images on a supported Debian release, starting with base images shared by many teams, or buy extended support for a fixed period where an upgrade has to wait.
Further reading	Debian announcement

Python 3.10 reaches end of life

Status	End of life, 1 October 2026
Who it affects	Services, serverless functions, container images and continuous integration jobs that still run Python 3.10.
What changes	Python 3.10.22 is the final release, and the 3.10 series receives no further security updates.[17]
Thirty-minute check	`grep -rnE 'python:3\.10|python3\.10|python-version:.*3\.10' .` in your repositories, and list serverless functions on the python3.10 runtime.
Recommended action	Move each service to a supported Python release, starting with internet-facing services and shared base images.

Further reading	Python 3.10.22 release notes

Kubernetes 1.34 out of maintenance

Status	End of maintenance, 27 October 2026
Who it affects	Self-managed clusters on Kubernetes 1.34. Managed Kubernetes services publish their own support calendars.
What changes	The Kubernetes project stopped publishing patch releases for 1.34 on 27 October 2026. The maintained releases are now 1.35, 1.36 and 1.37, and 1.35 follows on 28 February 2027.[19]
Thirty-minute check	`kubectl version -o json | jq -r .serverVersion.gitVersion` on every cluster.
Recommended action	Plan the upgrade to 1.35 or later, and move node images to cgroup v2 first, since 1.35 refuses cgroup v1 nodes by default.
Further reading	Kubernetes releases

Dated changes through 2029

macOS 14 runner image retired from GitHub Actions

Status	Retired 2 November 2026; last brownouts on 29 and 30 October 2026
Who it affects	Teams that build iOS, macOS or desktop applications on GitHub-hosted macOS runners.

What changes	GitHub retires the macOS 14 runner image on 2 November 2026. Jobs that use the `macos-14`, `macos-14-large` and `macos-14-xlarge` labels fail on purpose during scheduled brownouts between 5 and 31 October 2026. The last two brownouts run on 29 and 30 October 2026, from 14:00 to 24:00 Coordinated Universal Time.[20]
Thirty-minute check	`grep -rnE 'runs-on:.*macos-14' .github/workflows/` in every repository.
Recommended action	Move the jobs to `macos-15` or `macos-latest`, and confirm Xcode and toolchain versions on the new image before the next brownout.
Further reading	GitHub changelog

.NET 8 and .NET 9 reach end of support

Status	End of support, 10 November 2026
Who it affects	Teams that run services, functions or container images on .NET 8 or .NET 9.
What changes	Microsoft ends support for .NET 8 and .NET 9 on 10 November 2026. After that date it no longer provides servicing updates, security fixes or technical support for either version. .NET 10 is a long-term support release, supported until 14 November 2028.[23]
Thirty-minute check	`grep -rnE 'net(8|9)\.0' --include='*.csproj' .` and `grep -rnE 'dotnet/.*:(8|9)\.0' --include='Dockerfile*' .` in your repositories.
Recommended action	Move each service to .NET 10, starting with internet-facing services and shared base images.

Further reading	Microsoft .NET blog

European Union Product Liability Directive covers software

Status	Covers products placed on the market after 8 December 2026; transposition by 9 December 2026
Who it affects	Manufacturers of software, connected devices and products that contain software, sold in the European Union, including software supplied as a service.
What changes	Directive (EU) 2024/2853 applies to products placed on the market or put into service after 8 December 2026, and Member States must transpose it by 9 December 2026. Software counts as a product whatever the mode of supply or use, including software supplied as a service, and a manufacturer cannot escape liability for a defect caused by a software update, or by a missing update needed to maintain safety, when the update was within its control.[22]
Thirty-minute check	List the products and software versions you will place on the European Union market after 8 December 2026, and confirm that you can show which security updates each version received and when.
Recommended action	Keep release records, a software bill of materials and the update history for every version. Courts can order disclosure of evidence, and a failure to disclose leads to a presumption that the product is defective.
Further reading	European Commission: new liability rules

Let's Encrypt default certificates shortened to 64 days

Status	Starts 10 February 2027

Who it affects	Teams that use Let's Encrypt certificates, especially where renewal jobs run on a fixed schedule or wait until a fixed number of days before expiry.
What changes	From 10 February 2027 every certificate that Let's Encrypt issues or renews by default is valid for 64 days, and the authorization reuse period falls from 30 days to 10 days. The staging environment issues 64-day certificates from 14 October 2026 for testing.[24]
Thirty-minute check	Search renewal scripts, scheduled jobs and client configuration for fixed renewal thresholds, then run one renewal against the Let's Encrypt staging environment.
Recommended action	Renew at about two thirds of the certificate lifetime or use ACME Renewal Information, and monitor expiry separately from renewal.
Further reading	100-day certificates: automation plan

Public security certificates limited to 100 days

Status	Starts 15 March 2027
Who it affects	Every organisation with public certificates. Manual uploads, appliances, pinned certificates and partner connections carry the most risk.
What changes	Maximum validity falls from 200 to 100 days, and then to 47 days on 15 March 2029, when domain validation reuse also falls to 10 days.[8]
Thirty-minute check	Pull your certificates from Certificate Transparency logs with crt.sh and mark which ones renew automatically.

Recommended action	Move every certificate to the ACME protocol with automated domain validation, and monitor expiry separately from renewal.
Further reading	100-day certificates: automation plan

European Union Artificial Intelligence Act: high-risk obligations postponed

Status	Adopted; applies 2 December 2027 and 2 August 2028
Who it affects	Providers and deployers of high-risk artificial intelligence systems, including systems built into regulated products.
What changes	Regulation (EU) 2026/1744, in force since 27 July 2026, moves obligations for Annex III high-risk systems to 2 December 2027 and for Annex I systems (artificial intelligence in regulated products) to 2 August 2028. Providers of generative systems placed on the market before 2 August 2026 have until 2 December 2026 to mark generated content.[11]
Thirty-minute check	Do you have a list of the artificial intelligence systems you build or deploy, with an owner and a risk classification for each?
Recommended action	Continue the inventory and documentation work. The deadline moved, and the obligations remain.
Further reading	Model lineage and the Artificial Intelligence Act dates

Cyber Resilience Act applies in full

Status	Applies 11 December 2027

Who it affects	Manufacturers of products with digital elements sold in the European Union.
What changes	Essential cybersecurity requirements, vulnerability handling, a software bill of materials, a support period of at least five years (unless expected use is shorter) and security updates kept available for at least 10 years.[16,21]
Thirty-minute check	Can you state the support period for each product you will sell after December 2027, and show how updates will reach devices for that period?
Recommended action	Design the support period, the software bill of materials and the update path now, since they take longer than the documentation.
Further reading	Cyber Resilience Act reporting and Yocto Kirkstone

Items to watch

These deadlines are open or still moving. Each one can change cost, build time or contract requirements with little notice.

Cybersecurity Maturity Model Certification, Phase 2 suspended

Status	Suspended 13 July 2026; no restart date announced
Who it affects	Contractors and suppliers of the United States Department of Defense that handle Controlled Unclassified Information, including engineering and device companies deep in the supply chain.

What changes	Phase 2 would have required Level 2 certification by a third-party assessor in applicable solicitations and contracts from 10 November 2026. On 13 July 2026 the Department of War suspended Phase 2. Implementation remains in Phase 1, and its self-assessment requirements stay in place.[10]
Thirty-minute check	Check whether the contracts you hold or bid for include Level 1 or Level 2 self-assessment requirements, and whether the evidence behind your last self-assessment is still current.
Recommended action	Make access control, configuration management and audit logging produce evidence automatically from pipelines and infrastructure, so a restart of Phase 2 finds the evidence ready.
Further reading	Manufacturing Dive: Phase 2 paused

GitHub Actions runner pricing

Status	To watch since 1 January 2026
Who it affects	Teams with heavy GitHub Actions use, especially on self-hosted runners.
What changes	GitHub reduced prices for GitHub-hosted runners by up to 39% from 1 January 2026. A planned platform charge of 0.002 dollars per minute for self-hosted runners was postponed after feedback, and it may return.[12]
Thirty-minute check	Multiply last month's self-hosted runner minutes by 0.002 dollars to see the exposure if the charge returns, and compare the new hosted prices.
Recommended action	Repeat the comparison of hosted and self-hosted runners. For some teams the answer changed this year.

Further reading	GitHub: 2026 pricing changes

Docker Hub pull limits

Status	Ongoing
Who it affects	Build runners behind shared network addresses, and clusters that pull public images without signing in.
What changes	Anonymous pulls are limited to 100 per six hours per network address, and signed-in Personal accounts to 200.[13]
Thirty-minute check	Search recent pipeline logs for `toomanyrequests`.
Recommended action	Sign in for pulls, and mirror the images you depend on into your own registry.
Further reading	Docker Hub usage and limits

One practice for this quarter

This item is a window, not a deadline. The before-and-after picture is easiest to rebuild while last year's Git history still reflects how teams work today.

Measure delivery before and after coding assistants

Status	Before your next budget cycle
Who it affects	Engineering leaders who have introduced coding assistants or plan to.
What changes	The 2025 DevOps Research and Assessment report links artificial intelligence adoption to higher throughput and lower delivery stability.[15] A before-and-after measurement shows where the gain went.

Thirty-minute check	Compare the median time from pull request opened to merged for this quarter with the same quarter last year.
Recommended action	Record five delivery numbers now, and measure them again every quarter.
Further reading	Coding assistants and your delivery baseline

What is still open

- Cybersecurity Maturity Model Certification Phase 2 was suspended on 13 July 2026 pending a review, and no restart date has been announced. It may return on a revised timeline or in a revised form.
- The GitHub charge for self-hosted runners was postponed without a new date, and it may return in a different form.
- Dates and figures reflect the sources as checked on 29 October 2026. Regulators and vendors sometimes adjust dates, which is why the radar is reviewed every month.

A note to forward to your team

Delivery Deadline Radar check

The radar lists 22 dated changes that affect software delivery: rules in force, tools past end of support and dates coming up. Several of them passed with nothing failing on the day.

Please run the thirty-minute check for each item that applies to us by [date] and reply with two numbers:
1. Items that apply to us
2. Items already closed

For each open item, add an owner and a date.

Owner: [name]
Note: https://stonetusker.com/insights/delivery-deadline-radar.html

Using the radar in planning

Once a quarter, one person runs the checks for the items that apply and places each open item in the roadmap with a date and an owner. It takes an afternoon. For a wider view of where work waits between a commit and production, see the 20-Minute Delivery Checkup.

The next edition is planned for January 2027, with monthly reviews in between. New editions appear through the Stonetusker newsletters.

Questions

What is the Delivery Deadline Radar?

A quarterly list of dated changes that require action from engineering teams: regulations coming into force, tools reaching end of support and platform changes. Each item states

who it affects, a thirty-minute check and a recommended action.

Which items matter most for embedded and device companies?

Cyber Resilience Act reporting (since 11 September 2026), Yocto Kirkstone end of support, the end of Debian 11 long-term support, the Product Liability Directive for products placed on the market after 8 December 2026, the 2026 minimum elements for a software bill of materials, and full application of the Cyber Resilience Act on 11 December 2027.

Which items matter most for cloud and platform teams?

Ingress NGINX end of support, the Bitnami catalog change, cgroup v1 in Kubernetes 1.35, Kubernetes 1.34, which left maintenance on 27 October 2026, the removal of Node 20 from GitHub runners, .NET 8 and .NET 9 end of support on 10 November 2026, 64-day Let's Encrypt certificates from 10 February 2027 and 100-day public certificates from 15 March 2027.

How often is the radar updated, and how are dates checked?

The radar is reviewed every month and published as a new edition every quarter; the next edition is planned for January 2027. Each date is checked against at least two sources, with priority to the official project, regulator or vendor. Suspended or provisional items are marked as such.

Your personal radar

Run the checks for the items that apply first. If you would like a personal radar, reply with your stack and markets in a few words: cloud or devices, European Union or United States customers, Kubernetes or other platforms. No names, configuration or other internal details are needed. Within five working days you receive a short written list of the radar items that apply to you, in priority order, with the first action for each. It is free and confidential, and a call is optional.

Request your personal radar

The button opens an email to subeesh@stonetusker.com with the subject and the numbers to fill in. You can also use the contact page, or reply to the email or LinkedIn message that brought you here.

Next page for your situation

- Five-minute checklist for your archetype: eight plain questions and the dates that matter for your kind of product.
- 20-Minute Delivery Checkup: five numbers that show where your delivery waits.

Sources

1. European Commission: Cyber Resilience Act reporting obligations
2. Help Net Security: CISA sets a new SBOM baseline (July 2026)
3. Kubernetes Steering and Security Response Committees: Ingress NGINX statement
4. endoflife.date: Yocto Project release support dates
5. Bitnami: Upcoming changes to the Bitnami catalog
6. GitHub: Deprecation of Node 20 on GitHub Actions runners
7. Kubernetes enhancement proposal 5573: remove cgroup v1 support
8. DigiCert: TLS certificate lifetimes will officially reduce to 47 days
9. Cyber Resilience Act, Article 64 (penalties)

10. Department of Defense Chief Information Officer: About CMMC
11. Official Journal of the European Union: Regulation (EU) 2026/1744 (Digital Omnibus on artificial intelligence)
12. GitHub: 2026 pricing changes for GitHub Actions
13. Docker: Docker Hub usage and limits
14. env zero: What the CDKTF deprecation means for you
15. Google Cloud: Announcing the 2025 DORA Report
16. European Commission: Cyber Resilience Act
17. Python: Python 3.10.22, final release of the 3.10 series
18. Debian: Debian 11 long-term support reaches end of life
19. Kubernetes: Releases and support dates
20. GitHub: macOS 14 runner image retirement
21. Cyber Resilience Act, Article 13 (support period)
22. Official Journal of the European Union: Directive (EU) 2024/2853 on liability for defective products
23. Microsoft: .NET and .NET Core support policy
24. Let's Encrypt: 64-day certificate lifetimes coming February 2027 (7 October 2026)
25. Broadcom: How to prepare for the Bitnami changes coming soon (18 August 2025, updated)

About the author

Subeesh Sivanandan is the Founder and CEO of Stonetusker Systems. He has worked for more than 27 years in release engineering, DevOps, platform engineering & embedded Linux. His career includes serving as the Principal Engineer & Manager of Release Engineering at Stryker, alongside earlier roles at Nokia, VeriSign, and IP Infusion. LinkedIn profile.

Revision history (recent 3 updates)

Version 2.1, 29 October 2026. Every fact on this page is checked against a minimum of two sources each month.

Version	Date	Change
1.7	16 October 2026	Rewritten as an article for quick readers: introduction, summary of all major changes, what it means and first steps; one figure; commands folded for platform leads; print option and direct email offer
2.0	25 October 2026	Simpler layout and shorter text; all 22 items re-checked, with the remaining macOS 14 brownout dates added; the personal radar offer now asks for a few words about stack and markets only
2.1	29 October 2026	Kubernetes 1.34 moved to already past; last macOS 14 brownouts; Product Liability Directive wording aligned; links to the five checklists; email offer and next pages