Cyber Resilience Act Reporting Has Started and Yocto Kirkstone Is Out of Support: Check Your Products in 30 Minutes

Since 11 September 2026, manufacturers must send an early warning within 24 hours of becoming aware that a vulnerability in their product is actively exploited. Yocto 4.0 Kirkstone, still common in shipping devices, has had no updates since April 2026. This note shows how to check each product line and what to fix first.

For: Teams that ship firmware, devices or software products into the European Union.

Skip if: You sell nothing in the European Union, or your products fall under the European Union rules for medical devices, in vitro diagnostics or vehicle type approval, which the Cyber Resilience Act excludes.

By Subeesh Sivanandan, Founder, Stonetusker Systems · Updated 29 October 2026 · About 3 minutes to read · PDF version

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

The short version

- Since 11 September 2026, manufacturers must send an early warning within 24 hours of becoming aware that a vulnerability in their product is actively exploited, and a full notification within 72 hours.[1]
- The duty covers products already on the European Union market. Reports go through the Single Reporting Platform of the European Union Agency for Cybersecurity (ENISA).[3,4]
- Yocto 4.0 Kirkstone reached end of support in April 2026, so every security fix on it is now your own work.[6]
- A 24-hour warning is realistic only if you can name the affected products and firmware versions within hours, from stored records.

24 hours

To send an early warning after becoming aware of active exploitation[1]

April 2026

End of support for Yocto 4.0 Kirkstone[6]

2.5% of turnover

Or 15 million euros, whichever is higher, the maximum fine for these obligations[8]

A note to forward to your team

Cyber Resilience Act reporting and our Yocto base

Since 11 September 2026 we must send a 24-hour early warning and a 72-hour notification when a vulnerability in a product we sell in the European Union is actively exploited. Yocto Kirkstone has been out of support since April 2026.

Please run the four checks in this note for every product line by [date] and reply with three numbers:
1. Product lines that ship on Kirkstone or older
2. Shipped releases with a stored software bill of materials
3. Shipped releases without one

Reporting owner: [name]
Note: https://stonetusker.com/insights/cra-reporting-yocto-kirkstone.html

Why it matters now

The Cyber Resilience Act (Regulation (EU) 2024/2847) applies in stages.[2] Its reporting part has applied since 11 September 2026. An early warning is due within 24 hours, a full notification within 72 hours, and a final report no later than 14 days after a corrective measure is available (one month for a severe incident).[1] When a manufacturer first becomes aware of active exploitation after 11 September 2026, the duty applies, even if the vulnerability itself was known earlier.[4]

Consider a library such as OpenSSL reported as exploited on a Friday afternoon. Someone must know which shipped products and firmware versions contain it. If that answer needs a rebuild of an old tag, the 24 hours pass first.

An unsupported Yocto base makes the next part harder. Each fix means finding the upstream patch, backporting it, rebuilding, testing and shipping. The main obligations

apply from 11 December 2027, including a support period of at least five years unless the expected use is shorter.[2,5]

Check each product line in 30 minutes

Step 1. Find the Yocto release series

Open the build tree of the release that is currently shipping and run:

```
grep -r --include=layer.conf LAYERSERIES_CORENAMES .
```

The core layer names the series, for example `kirkstone` or `scarthgap`. If you use kas or repo manifests, the branch names in the manifest show the same information.

Step 2. Look for a stored software bill of materials

Open the release archive of the shipped firmware version and look for the software bill of materials that the build produced. Note whether it exists for every shipped release, or whether you would need a rebuild to produce one.

Step 3. Name the reporting owner

Write down who decides to send an early warning, and whether that person already has access to the Single Reporting Platform.

Step 4. Measure the update path

Write down how a fixed build reaches devices in the field, and how long that takes from merged fix to updated device.

What the result means

What you find	What it means	Typical effort
Scarthgap (supported until April 2028) or Wrynose (supported until April 2030), with a stored software bill of materials for each release	Security fixes arrive through Yocto point releases, and you can answer exposure questions from records	Monitoring and a rehearsal
Kirkstone or older, with a stored software bill of materials for each release	You can find exposure quickly, and every fix is a manual backport	An upgrade plan per product line
Kirkstone or older, without stored software bills of materials	The 24-hour warning depends on memory and rebuilds	Regenerate them first, then plan the upgrade

Release support dates come from the Yocto Project.[6] Chip vendor board support packages often decide which release you can move to and when.

The move, step by step

1. **Name the reporting owner.** Decide who submits an early warning, arrange access to the Single Reporting Platform and write a one-page runbook.
2. **Archive a software bill of materials for every shipped build.** Enable generation in the build (create-spdx) and store the output with each release. Regenerate older releases still in the field once from their tags.
3. **Monitor vulnerabilities daily.** Check the stored records against public feeds, including the Known Exploited Vulnerabilities catalog of the United States Cybersecurity and Infrastructure Security Agency.
4. **Decide the path for each Kirkstone product.** Upgrade to Scarthgap or Wrynose, buy extended maintenance for a fixed period, or set an end-of-sale date, and record the decision with a date.

5. **Rehearse against the clock.** Take a real earlier vulnerability and run the whole process against 24 hours. Improve the slowest step first.

Wrynose makes SPDX 3.0 the only format for the software bill of materials it generates, which records build relationships and supports statements about which vulnerabilities do not affect you.[7]

What is still open

- The European Commission may still publish implementing acts and guidance, including on the format of the software bill of materials.
- National authorities are building their enforcement practice, so the first cases will clarify details.
- Chip vendors decide when board support packages for newer Yocto releases appear.

Questions

What are the reporting deadlines?

An early warning within 24 hours of becoming aware, a notification within 72 hours, and a final report within 14 days after a corrective measure is available for a vulnerability, or within one month for a severe incident.

Does the duty cover products already on the market?

It covers products already placed on the European Union market. Exploitation the manufacturer knew about before 11 September 2026 need not be reported retrospectively. Awareness after that date triggers the duty.

When did Yocto Kirkstone reach end of support?

In April 2026, at the end of its four-year long-term support period. Scarthgap (5.0) is supported until April 2028 and Wrynose (6.0) until April 2030.

What are the penalties?

Breaches of the essential requirements or of the manufacturer obligations in Articles 13 and 14 can lead to fines of up to 15 million euros or 2.5% of total worldwide annual

turnover, whichever is higher.

Want a second opinion?

Run the check yourself first. If you would like a second opinion, reply with two counts only: the products that ship on Kirkstone and the shipped releases with a stored software bill of materials. No product names, configuration, files or build output are needed. Within five working days you receive a short written review with what reporting needs now, what to prepare before December 2027 and a realistic path off Kirkstone. It is free and confidential, and a call is optional.

Ask for a second opinion

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

- European Union dates for device makers: the other European Union rules with dates in 2026 and 2027, in one table.
- 2026 software bill of materials elements: what a complete component record now contains.

Sources

1. European Commission: Cyber Resilience Act reporting obligations
2. European Commission: Cyber Resilience Act
3. ENISA: Single Reporting Platform
4. ENISA: Single Reporting Platform, frequently asked questions
5. Cyber Resilience Act, Article 13 (support period)

6. Yocto Project: Releases
7. Yocto Project: Migration notes for release 6.0 (Wrynose)
8. Cyber Resilience Act, Article 64 (penalties)

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
1.4	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; the review offer now asks for a few counts only
2.1	29 October 2026	Who-this-is-for box, note to forward moved up, email offer with the numbers listed, and next pages including the European Union dates page