PRODUCT CYBERSECURITY

XP Power and the **EU Cyber Resilience Act**

Position statement - Regulation (EU) 2024/2847

Field	Detail
Version	1.1, published 11 September 2026
Review	Reviewed at least once a year, owned by XP Power Product Security. Next review due by 10 September 2027.
Issued by	X P PLC, registered in England & Wales at 16 Horseshoe Park, Pangbourne, Berkshire RG8 7JW, United Kingdom. Registration number 02297983. XP Power is a trading name of X P PLC.

This statement explains what Regulation (EU) 2024/2847, the Cyber Resilience Act, requires of manufacturers, how it applies to XP Power's products, and what XP Power is doing about it. It is written for customers, distributors and compliance teams who need an answer they can file.

For how to report a suspected vulnerability in an XP Power product, see our Coordinated Vulnerability Disclosure Policy at https://www.xppower.com/product-cybersecurity. That is a separate document and it takes precedence on anything to do with reporting.

1. What the Cyber Resilience Act is

The Cyber Resilience Act is an EU regulation that sets cybersecurity requirements for products with digital elements placed on the EU market. It covers hardware and software, and it covers the whole product lifecycle rather than the moment of sale. From the date it applies in full, conformity with it becomes a condition of CE marking, alongside the existing directives.

It does two things that matter to a power supply manufacturer. It requires products to be designed and maintained to a security baseline. And it requires manufacturers to report actively exploited vulnerabilities and severe incidents to the authorities, on a fixed clock, whether or not the product is new.

2. When it applies

The Regulation sets three application dates. It entered into force on 10 December 2024, and a fourth date applies to legacy approvals: EU type-examination certificates and approval decisions on cybersecurity issued under other Union harmonisation legislation remain valid until 11 June 2028. These dates are taken from the Regulation as published in the Official Journal.

Date	What applies
11 June 2026	Chapter IV, Articles 35 to 51 - the designation of conformity assessment bodies and notified bodies
11 September 2026	**Article 14, the reporting obligations on manufacturers**
11 December 2027	The rest of the Regulation, including the essential requirements, technical documentation, support periods and CE marking

The September 2026 date is the one that is often misread. It does not affect CE marking, which becomes conditional on conformity with the Regulation from 11 December 2027. What it does is start the reporting clock, and that obligation stands on its own: failure to comply with Article 14 sits in the highest penalty tier under Article 64(2), alongside breach of the essential requirements. From that date, a manufacturer that becomes aware of an actively exploited vulnerability in one of its products, or of a severe incident affecting the security of one of its products, must notify the CSIRT designated as coordinator and ENISA simultaneously, through the EU single reporting platform, as follows:

Stage	Actively exploited vulnerability	Severe incident
Early warning	Without undue delay, and in any event within **24 hours** of becoming aware	Without undue delay, and in any event within **24 hours** of becoming aware
Notification	Without undue delay, and in any event within **72 hours** of becoming aware	Without undue delay, and in any event within **72 hours** of becoming aware
Final report	No later than **14 days** after a corrective or mitigating measure is available	Within **one month** of submitting the notification

The 24 and 72 hour figures are outer limits, not the duty: the duty is to report without undue delay. Note also the asymmetry in the final report, which is widely reproduced incorrectly. The obligation applies to

products already on the market, not only to new designs. Article 69(3) applies Article 14 to all in-scope products placed on the market before 11 December 2027, so the existing installed base is covered from 11 September 2026. Article 14 also requires the manufacturer to inform impacted users, and where appropriate all users, of the vulnerability or incident and of any corrective or mitigating measures, where necessary in a structured, machine-readable format. Reporting to the authorities does not discharge that duty.

Reporting is made through the single reporting platform established under Article 16 and operated by ENISA, which is scheduled to be operational from 11 September 2026. Platform availability does not suspend the deadlines, which run from the point of becoming aware. Where the platform is unavailable, ENISA's guidance is to contact the designated CSIRT directly in urgent cases and to submit through the platform once it is available.

3. Which businesses the Regulation applies to, and what counts as a digital product

Article 2 applies the Regulation to products with digital elements made available on the EU market, and Chapter II places the obligations on manufacturers, with separate duties for importers and distributors. The test that decides the matter for power conversion products is the scope condition in Article 2(1): whether the product's intended purpose or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network. Note that this is a condition of scope, not part of the definition of a product with digital elements at Article 3(1).

XP Power applies that test as follows. This is our reading of the Regulation, and it is consistent with positions published elsewhere in this industry.

Counts as a data connection	Does not count
PMBus, I²C, SMBus	DC-OK, AC-OK, power-good
CAN and CANopen	Remote on/off, inhibit, enable
Modbus RTU, RS-485, RS-422, RS-232, UART	Analogue programming (0-5 V, 0-10 V), voltage trim
Ethernet / TCP-IP, EtherCAT, DeviceNet, Profibus DP	Current monitor and analogue monitor outputs
USB (data), GPIB / IEEE-488, and SCPI over any of the above	Parallel operation and current-share signals, fault relay contacts, LED indicators

A product can contain a digital element - a microcontroller used for internal sequencing or protection - and can still fall outside the Regulation, because it has no data connection. That distinction decides most of a power supply portfolio, and it is the boundary we expect to have to evidence.

4. What this means for XP Power's products

A growing number of XP Power products fall within the scope of the Regulation, and we expect that number to keep growing. More of our range is designed with digital communication and control rather than analogue signalling alone. This is not something we treat as marginal, or as settled.

The families we have confirmed as **in scope** so far, because XP Power's own literature documents a digital interface, are **HPx, FLXPro, nanofleX, GFR1K5, and our high-voltage supplies used with a digital interface module.** Further families are under review and we expect to add to this list. We are also determining separately how the PC software supplied to configure and monitor these products is treated.

Products that provide only analogue programming, monitoring and binary status signals, with no data connection in the sense of section 3, are outside the scope. We are confirming that family by family against our own published specifications rather than by assumption, and the determination is not complete.

If you need the position for a specific part number, ask us. We will give you the determination and the reasoning behind it. We intend to publish the result per product so that the question can be answered without contacting us, and we will say when.

5. XP Power's approach

Report first. Article 14 applies from 11 September 2026, so the reporting route came first. From the date of this statement XP Power provides separate product security and infrastructure security reporting routes with a published mailbox for each, a published Coordinated Vulnerability Disclosure Policy, a web form that accepts anonymous reports, published OpenPGP keys with their fingerprints so that a report can be encrypted, and machine-readable contact details in a cryptographically signed security.txt. Those exist so that a researcher or a customer can reach us, and so that a report is recorded and acted on.

Scope next. The determination described in section 4, family by family, against our own published specifications rather than by assumption.

Then the December 2027 requirements. Secure development and update processes, the technical documentation, stated support periods and the conformity assessment route. This is engineering and product management work with a longer lead time than the reporting route, and it is the part XP Power is working on now.

How we handle a report. Every report is assessed, and a case is never closed on one person's judgement alone. Where an XP Power product is subject to an actively exploited vulnerability we notify the CSIRT designated as coordinator and ENISA simultaneously and without undue delay, coordinate the timing of any disclosure with the CSIRT, and inform affected users. Our response times, our disclosure timescales and the conditions on which we close a case are all set out in the Coordinated Vulnerability Disclosure Policy.

6. What XP Power is not claiming

We would rather be precise than reassuring, so it is worth being clear about what this statement does not say.

- **It does not claim that XP Power products are CRA-compliant.** Conformity is assessed against the essential requirements that apply from December 2027. That work is under way and it is not finished.
- **It does not claim certification to any cybersecurity standard.** Where XP Power adopts a standard as its working basis we will say which one, and we will say whether it is a target or an assessed position.
- **It does not state support periods or update availability.** A published support period is a commitment across an installed base, and we will publish it when we can stand behind it family by family, not before.
- **It does not make a scope claim for any individual part number.** Section 4 describes the shape of the portfolio and names the families confirmed so far. The per-product answer comes from the determination in progress.

Where a question here matters to a design you are working on, ask us. An honest answer with its reasoning is more useful than a claim.

7. Reporting a vulnerability

Route	Address
Product vulnerabilities	psirt@xppower.com
XP Power infrastructure	csirt@xppower.com
Report page and web form, including anonymous reports	https://www.xppower.com/product-cybersecurity
Machine-readable contact details, signed	https://www.xppower.com/.well-known/security.txt

8. Contact

XP Power Product Security
psirt@xppower.com
+44 (0)118 984 5515 Monday to Thursday 08:00 to 17:30, Friday 08:00 to 15:00, UK time

Product cybersecurity information, including our Coordinated Vulnerability Disclosure Policy and our OpenPGP keys: https://www.xppower.com/product-cybersecurity

The Regulation itself: Regulation (EU) 2024/2847 of the European Parliament and of the Council, done at Strasbourg on 23 October 2024. The text as published in the Official Journal is at https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng