XP Power

PRODUCT CYBERSECURITY

Coordinated Vulnerability Disclosure Policy

Field	Detail
Version	Interim version 1.0
Published	11 September 2026
Effective	11 September 2026
Review	Reviewed at least once a year. Next review due by 11 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.

An interim policy to open XP Power's vulnerability reporting route. A fuller version will replace it. The channels, response times and assurances below take effect on 11 September 2026. We do not intend to weaken them in any later version.

1. Scope

XP Power welcomes reports of suspected cybersecurity vulnerabilities in its products, from anyone.

In scope: cybersecurity vulnerabilities in XP Power products and in the software, firmware, communication interfaces, configuration tools and update mechanisms supplied with them or supplied separately, including software we make available to download, and products with digital elements placed on the market under the XP Power brand. Also XP Power's own infrastructure.

Out of scope: general technical support, availability and commercial enquiries; corporate IT matters unrelated to our products or infrastructure; vulnerabilities in third-party services we do not operate.

What counts as a valid vulnerability. It affects an XP Power product or our infrastructure; it relates to information not already publicly known; and it is not the unsupported output of an automated scan. Automated findings are welcome with evidence that the finding is real. **A report failing these tests is still read and still answered.**

2. How to report

Route	Address
Product vulnerabilities	psirt@xppower.com **- preferred route**
XP Power infrastructure	csirt@xppower.com
Web form, including anonymous reports	https://www.xppower.com/product-cybersecurity
Telephone	+44 (0)118 984 5515 Monday to Thursday 08:00 to 17:30, Friday 08:00 to 15:00, UK time

We accept both email addresses and telephone numbers as contact details. Either one on its own is enough.

Please encrypt anything sensitive, and sign your message. Our OpenPGP keys:

psirt@xppower.com - https://www.xppower.com/.well-known/psirt.asc
fingerprint E6EE 9A58 FFEC 7301 C625 B0CA 3280 4FE1 21DB 4DA7
csirt@xppower.com - https://www.xppower.com/.well-known/csirt.asc
fingerprint 30EF 837B 6074 DABC D0EC F375 18DE 2678 E322 EE22

If you cannot retrieve a key, email us and we will send it.

If you would like our reply encrypted, send us your own public key or its fingerprint. Without it we can only reply in plain text.

Reporting anonymously. The web form accepts anonymous reports. Please understand the cost: **an anonymous report can only be processed to a limited extent, and may not be able to be processed at all**. We cannot ask a follow-up question, give you a named case owner, send you the response times in section 4, or tell you when the case closes. Complex issues usually need

explanation before we can act. Any contact route at all, even a pseudonymous one, takes the report further.

Useful to include: product, model, variant and version; what the vulnerability is and how to reproduce it; what an attacker could do; whether you have seen it exploited; any mitigation you have found; and whether you have told anyone else.

3. What we ask of you

- Act in good faith and avoid harm to XP Power, our customers, users and third parties.
- Do not exploit a vulnerability further than needed to show that it exists.
- Do not disrupt systems, services or customer operations. No denial-of-service testing, social engineering, phishing, spam or physical attacks.
- Do not access, change or disclose data that is not yours.
- Keep the details confidential until the disclosure described in section 5, or until we tell you the case is closed. We will not hold you to that indefinitely. If neither has happened within 90 days of your report, this request lapses, unless we have agreed a longer period with you.

These are the points the web form asks you to confirm. **If you cannot confirm them, report anyway**. Every report that reaches us is handled as fully as we are able to handle it. What you lose is the safe harbour in section 4 and public credit, not our attention.

We also ask that everyone involved treats everyone else with respect.

4. What we promise you

We will not require you to sign a non-disclosure agreement. Response times, unless you reported anonymously:

- **Within four working days**, a first response from a person. Not an automated acknowledgement.
- **Within ten working days**, considered feedback, being at least one of: confirmation of the vulnerability; rejection of it; the specific questions we need answered; or an explanation of why it is taking longer, with a commitment to update you again within a further ten working days.

Confidentiality. Every report is confidential so far as the law allows, the exception being information that has to appear in the public disclosure in section 5. **We will not disclose your personal data to any third party without your explicit consent, unless we are required to disclose it by law**. Access inside XP Power is limited to those who need it to investigate, fix, coordinate disclosure or meet a legal obligation. We may need to share vulnerability information, and, unless the law requires otherwise, not your identity, with an affected supplier or customer, the CSIRT designated as coordinator, ENISA or a market surveillance authority, where that is necessary to reduce risk or required of us by law.

Your personal data. X P PLC is the controller for personal data you send us. We use it only to handle your report, to coordinate disclosure and to meet our legal obligations, and we keep it for as long as those purposes require. Our privacy notice is at https://www.xppower.com/privacy and it explains your rights and how to exercise them. You can report anonymously if you prefer, on the terms in section 2.

Safe harbour. Where you have complied with section 3 of this policy, XP Power will not bring or support a civil claim against you, and will not make a criminal complaint about you, in respect of your research. If someone else brings an action against you over a report you made in accordance with this policy, we will confirm that your conduct complied with it. **We cannot prevent action by a prosecuting authority or by a third party, and this assurance is not legal advice**. It does not apply where you have acted for extortion or personal gain.

We stay reachable. A named case owner is your contact for the whole process, and questions about progress are welcome at any point.

Reports of already-fixed issues. Send them anyway. We read and check them.

5. Disclosure

We publish a validated and verified vulnerability **within 90 days**. Where a fix or mitigation is taking longer for good reason, that may be extended once by a further 90 days in consultation with the CSIRT designated as coordinator, and beyond that only with that CSIRT's agreement. Where we find and fix a vulnerability before the product reaches the market, there is nothing to disclose.

We request publication on the **European Vulnerability Database** maintained by ENISA, in consultation with the CSIRT designated as coordinator, and may also publish our own advisory naming the affected products, the impact, a severity rating and the fix.

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, and coordinate our mitigation and its timing with that CSIRT. Where an actively exploited vulnerability or a severe incident affects an XP Power product, we also inform the impacted users, and where appropriate all users, of the vulnerability or incident and of any mitigation they can apply.

If you would like to be credited, tell us, and we will agree the name or alias with you before anything is published.

6. When a case is closed

We close a case, and tell you we have closed it unless you reported anonymously, when any of the following is true:

- The report turns out to be unfounded.
- The vulnerability has been fixed or mitigated and has been publicly disclosed.
- The vulnerability was in a service, and that service has been fixed and the vulnerability disclosed.
- You have not answered our technical questions for 30 days or more, so the report cannot be taken further.
- The vulnerability has been publicly disclosed and, in consultation with the CSIRT designated as coordinator, it can no longer be assumed that it will be fixed or mitigated.

No case is closed on one person's judgement alone.