DEVICE INSIGHT

COORDINATED VULNERABILITY DISCLOSURE

Policy of Device Insight GmbH

Version: 2 October 2026

1. Scope of this policy

If you discover a vulnerability in an IT product, IT system or IT service of Device Insight, you can contact us directly. Every report is reviewed, regardless of the channel through which it reaches us.

This policy applies to products and systems that Device Insight develops, operates or distributes under its own name. If your report concerns a product that was developed on behalf of a customer and placed on the market under that customer's brand, the customer is the manufacturer and the appropriate point of contact. In such cases, Device Insight provides support in the background.

2. If another manufacturer is affected

If the vulnerability concerns a product, system or service of another manufacturer or party responsible for the product, please report it there first. If that manufacturer does not respond, or if the vulnerability disclosure process is at risk of breaking down without a response, you may contact Device Insight. We will then assess how we can support you.

3. Process and basis

A report is taken into our CVD process only if the points set out in Section 9 have been observed. How Device Insight handles vulnerability reports internally is governed by a separate process document; the commitments relevant to you as a reporter are summarised in this policy.

4. What your report should contain

To allow us to assess and remediate a vulnerability quickly, your report should include the following:

- The affected product or system, including version or configuration where known.
- A description of the vulnerability and its impact.
- Steps to reproduce the issue or a proof of concept, where available.
- Details of the test environment used and of any measures already taken.
- An email address for follow-up questions.

Reports consisting solely of automated scan output without further explanation cannot be processed as valid reports (see Section 9).

5. Our commitments

- We treat every vulnerability report as confidential within the limits of applicable law.
- We do not disclose personal data to third parties without your explicit consent.
- We acknowledge receipt of your report within 3 working days.
- We keep you informed about the status of your report while it is being processed.
- To the extent permitted by law, Device Insight will neither file a criminal complaint nor submit a criminal application, and will not assert its own civil claims in relation to vulnerability research conducted in good faith and in accordance with this policy. This commitment applies only to claims of Device Insight GmbH. Rights of third parties and actions by governmental authorities remain unaffected. This commitment does not apply to intentionally unlawful or abusive conduct, including exploitation of a vulnerability, unauthorized access to data, system manipulation, or harm to third parties.
- A dedicated contact person is available to you throughout the entire process.
- We inform you as soon as a fix is available and agree with you which information about it will be published.

6. Recognition and remuneration

Device Insight does not operate a bug bounty program. We do not pay bounties, remuneration or reimbursement of expenses for vulnerability reports, and there is no entitlement to any such payment. We nonetheless value the work of security researchers and will agree with you whether you wish to be credited as the reporter when information about the vulnerability is published.

7. Disclosure and embargo

Until a vulnerability has been remediated, we treat all information about it as confidential and ask you to exercise the same restraint towards third parties and the public.

As a standard, an embargo period of 90 days applies, starting from our acknowledgement of receipt. Within this period we develop and release a fix; afterwards we agree with you which information about the vulnerability will be published, for example as part of the fix information referred to in Section 5.

If a fix becomes available before the 90 days have elapsed, we publish the information promptly and in coordination with you. If remediation requires more time, for instance in the case of complex systems or where customers need additional lead time for deployment, we extend the period by mutual agreement.

If no agreement has been reached by the end of the 90 days, you are free to disclose the vulnerability thereafter. We ask that you notify us beforehand.

For actively exploited vulnerabilities or comparably critical cases, the period may differ: here, protecting affected users takes precedence over the standard period.

8. Data protection

If your report or the reporting form contains personal data, our privacy notice applies. Information on how security-related reports are handled can be found there in the section headed “Information Security”.

https://device-insight.com/en/privacy/

9. What we expect from you

- The vulnerability has not been exploited. No damage was caused beyond the discovery of the vulnerability itself.
- No attacks were carried out against IT systems or infrastructure, such as social engineering, spam, (distributed) denial-of-service or brute-force attacks.
- No third-party systems or data were manipulated, compromised or altered.
- No tools for exploiting the vulnerability were offered, whether for payment or free of charge, for instance on darknet marketplaces.
- The report does not consist solely of automated scan output without explanatory documentation. Raw tool output without further assessment does not constitute a valid report.
- The reported vulnerability was not previously known. We accept and review information on vulnerabilities that have already been remediated, but such reports are not processed further within the CVD process.
- You provide a valid email address. Particularly with more complex vulnerabilities, we frequently need to ask follow-up questions or request additional documentation. Without a means of contact, we can process a report only to a limited extent.

Please note for anonymous reports: technical follow-up questions from Device Insight or the affected manufacturer cannot be answered. Processing is therefore limited and may not be possible in individual cases.

10. Contact

Device Insight GmbH

Willy-Brandt-Platz 6

81829 Munich, Germany

Phone: +49 (0) 89 4545448-22

Email: infosec-incident@device-insight.com

Encryption (recommended): Please encrypt sensitive reports using our OpenPGP key.

https://keys.openpgp.org/search?q=infosec-incident%40device-insight.com

Fingerprint: 5DDA 9894 53A0 86A9 C81B 0DDE 77EB 30D2 33BD 381C

11. Language

This document is a translation of the German original. In case of discrepancies, the German version prevails.