DEVICE INSIGHT

COORDINATED VULNERABILITY DISCLOSURE

Richtlinie der Device Insight GmbH

Stand: 02.10.2026

1. Worum es hier geht

Wer eine Schwachstelle in einem IT-Produkt, einem IT-System oder einer IT-Dienstleistung von Device Insight findet, kann sich direkt an uns wenden. Jede Meldung wird geprüft, unabhängig davon, auf welchem Weg sie eingeht.

Diese Richtlinie gilt für Produkte und Systeme, die Device Insight unter eigenem Namen entwickelt, betreibt oder vertreibt. Betrifft die Meldung ein Produkt, das im Kundenauftrag entwickelt wurde und unter der Marke des Kunden auf den Markt kommt, ist der Kunde als Hersteller der richtige Ansprechpartner. Device Insight unterstützt in solchen Fällen im Hintergrund.

2. Wenn ein anderer Hersteller betroffen ist

Betrifft die Schwachstelle ein Produkt, System oder eine Dienstleistung eines anderen Herstellers oder Produktverantwortlichen, melden Sie diese zunächst dort. Reagiert der Hersteller nicht oder droht der Vulnerability-Disclosure-Prozess ohne Reaktion abzubrechen, können Sie sich an Device Insight wenden. Wir prüfen dann, wie wir unterstützen können.

3. Ablauf und Grundlage

Eine Meldung wird nur dann in unseren CVD-Prozess übernommen, wenn die in Abschnitt 9 genannten Punkte eingehalten sind. Wie Device Insight intern mit Schwachstellenmeldungen umgeht, ist in einem eigenen Prozessdokument geregelt; die für Sie als Melder relevanten Zusagen sind in dieser Richtlinie zusammengefasst.

4. Was Ihre Meldung enthalten sollte

Damit wir eine Schwachstelle zügig einordnen und beheben können, sollte Ihre Meldung Folgendes enthalten:

- Das betroffene Produkt oder System, soweit bekannt inklusive Version oder Konfiguration.
- Eine Beschreibung der Schwachstelle und ihrer Auswirkung.
- Schritte zur Reproduktion oder einen Nachweis (Proof of Concept), soweit vorhanden.
- Angaben zur verwendeten Testumgebung und zu bereits ergriffenen Maßnahmen.
- Eine E-Mail-Adresse für Rückfragen.

Meldungen, die nur aus einer automatisierten Scan-Ausgabe ohne Einordnung bestehen, können wir nicht als gültige Meldung bearbeiten (siehe Abschnitt 9).

5. Das sichern wir zu

- Wir behandeln jede Schwachstellenmeldung im Rahmen des gesetzlich Zulässigen vertraulich.
- Wir geben personenbezogene Daten nicht ohne Ihre ausdrückliche Zustimmung an Dritte weiter.
- Wir bestätigen den Eingang Ihrer Meldung innerhalb von 3 Werktagen.
- Wir halten Sie während der Bearbeitung über den Status Ihrer Meldung auf dem Laufenden.
- Soweit gesetzlich zulässig wird Device Insight wegen einer Schwachstellenmeldung, die in gutem Glauben und im Einklang mit dieser Richtlinie erfolgt, weder Strafanzeige erstatten oder Strafantrag stellen noch eigene zivilrechtliche Ansprüche geltend machen. Dies gilt ausschließlich für Ansprüche der Device Insight GmbH. Rechte Dritter sowie Maßnahmen staatlicher Behörden bleiben unberührt. Die Zusage gilt nicht bei vorsätzlich rechtswidrigem oder missbräuchlichem Verhalten, insbesondere bei Ausnutzung einer Schwachstelle, unbefugtem Datenzugriff, Manipulation von Systemen oder Schädigung Dritter.
- Während des gesamten Prozesses steht Ihnen bei uns eine feste Kontaktperson zur Verfügung.
- Wir informieren Sie, sobald ein Fix verfügbar ist, und stimmen mit Ihnen ab, welche Informationen dazu veröffentlicht werden.

6. Anerkennung und Vergütung

Device Insight betreibt kein Bug-Bounty-Programm. Für Schwachstellenmeldungen zahlen wir keine Prämien, Vergütungen oder Aufwendungsersatz; ein Anspruch hierauf besteht nicht. Wir schätzen die Arbeit von Sicherheitsforschenden dennoch ausdrücklich und stimmen mit Ihnen ab, ob Sie bei der Veröffentlichung von Informationen zur Schwachstelle als Melder genannt werden möchten.

7. Offenlegung und Embargo

Bis eine Schwachstelle behoben ist, behandeln wir alle Informationen dazu vertraulich und bitten Sie um dieselbe Zurückhaltung gegenüber Dritten und der Öffentlichkeit.

Als Standard gilt eine Embargo-Frist von 90 Tagen ab der Eingangsbestätigung. Innerhalb dieser Frist entwickeln und veröffentlichen wir einen Fix; danach stimmen wir mit Ihnen ab, welche Informationen zur Schwachstelle veröffentlicht werden, etwa im Rahmen der in Abschnitt 5 zugesagten Fix-Informationen.

Ist ein Fix vor Ablauf der 90 Tage verfügbar, veröffentlichen wir die Informationen zeitnah gemeinsam mit Ihnen abgestimmt. Braucht die Behebung mehr Zeit, etwa bei komplexen Systemen oder wenn Kunden zusätzliche Vorlaufzeit für die Einspielung benötigen, verlängern wir die Frist im Einvernehmen mit Ihnen.

Kommt bis zum Ablauf der 90 Tage keine Einigung zustande, können Sie die Schwachstelle danach eigenständig offenlegen. Wir bitten Sie, uns vorher zu informieren.

Bei aktiv ausgenutzten Schwachstellen oder vergleichbar kritischen Fällen kann die Frist abweichen: Hier hat der Schutz betroffener Nutzer Vorrang vor der Standardfrist.

8. Datenschutz

Enthält Ihre Meldung oder das Meldeformular personenbezogene Daten, gelten unsere Datenschutzhinweise. Hinweise zum Umgang mit sicherheitsrelevanten Meldungen finden Sie dort im Abschnitt „Informationssicherheit“.

https://device-insight.com/datenschutz/

9. Das erwarten wir von Ihnen

- Die Schwachstelle wurde nicht ausgenutzt. Es entstand kein Schaden, der über das Auffinden der Schwachstelle hinausgeht.
- Es fanden keine Angriffe auf IT-Systeme oder Infrastrukturen statt, etwa Social Engineering, Spam, (Distributed) Denial-of-Service oder Brute-Force.
- Systeme oder Daten Dritter wurden weder manipuliert noch kompromittiert oder verändert.
- Es wurden keine Tools zur Ausnutzung der Schwachstelle angeboten, entgeltlich oder unentgeltlich, etwa auf Darknet-Marktplätzen.
- Die Meldung stammt nicht allein aus einem automatisierten Scan ohne erläuternde Dokumentation. Reine Tool-Ausgaben ohne Einordnung gelten nicht als gültige Meldung.
- Die gemeldete Schwachstelle ist bislang nicht bekannt. Hinweise zu bereits behobenen Schwachstellen nehmen wir entgegen und prüfen sie, sie werden aber nicht im CVD-Prozess weiterbearbeitet.
- Sie hinterlegen eine gültige E-Mail-Adresse. Gerade bei komplexeren Schwachstellen brauchen wir häufig Rückfragen oder zusätzliche Dokumentation. Ohne Kontaktmöglichkeit können wir eine Meldung nur eingeschränkt bearbeiten.

Bei anonymen Meldungen gilt: Fachliche Rückfragen von Device Insight oder dem betroffenen Hersteller können nicht beantwortet werden. Die Bearbeitung ist dadurch eingeschränkt oder im Einzelfall nicht möglich.

10. Kontakt

Device Insight GmbH

Willy-Brandt-Platz 6

81829 München

Telefon: +49 (0) 89 4545448-22

E-Mail: infosec-incident@device-insight.com

Verschlüsselung (empfohlen): Bitte verschlüsseln Sie sensible Meldungen mit unserem OpenPGP-Schlüssel.

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

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