



CRA-GEREEDHEIDSCHECK

Is vdhSensor klaar voor de Cyber Resilience Act?

Gapregister, meldprocedure en een eerste softwarestuklijst voor een verbonden product

vdhSensor BV, Heverlee (12 medewerkers, één product: een verbonden luchtkwaliteitsmeter)
Opgesteld op 20 oktober 2026

VOORBEELDUITTREKSEL - vdhSensor BV en haar product zijn fictief

De meldplicht geldt al; de meeste eisen pas vanaf 11 december 2027. Van de 21 punten in het gapregister zijn er 6 in orde, 9 deels en 6 niet. Voorrang hebben twee punten: een procedure om actief misbruikte kwetsbaarheden en ernstige incidenten op tijd te melden, wat al verplicht is, en een kanaal waar anderen kwetsbaarheden kunnen melden, wat pas vanaf december 2027 verplicht is maar nu al nodig is om misbruik op tijd te horen. Twee punten staan in dit uittreksel.

Inhoud van het volledige rapport

In het kort (in dit uittreksel)	2
1. Valt het product onder de CRA, en in welke klasse?	3
2. Gapregister	4
2.3 Melden van actief misbruikte kwetsbaarheden (in dit uittreksel)	5
2.6 Kanaal voor meldingen van buitenaf (in dit uittreksel)	6
3. Meldprocedure (ontwerp)	10
4. Eerste softwarestuklijst (SBOM)	13
5. Volgorde en planning tot december 2027	15

Het volledige rapport telt 16 pagina's. Dit uittreksel toont de samenvatting en twee bevindingen; de werkwijze, de volledige lijsten en de bijlagen staan alleen in het rapport voor de klant.

Dit is een voorbeelduittreksel. vdhSensor BV en haar product zijn verzonnen. De verwijzingen naar de Cyber Resilience Act (Verordening (EU) 2024/2847) zijn echt en op de datum hierboven gelezen in geconsolideerde teksten; de klasse van het product is een eerste inschatting, te bevestigen. Dit is geen conformiteitsbeoordeling en geen juridisch advies.

In het kort

vdhSensor verkoopt een luchtkwaliteitsmeter met wifi en een app, in België, Nederland en Frankrijk. Ik werkte met de CTO en de firmware-ontwikkelaar (twee werksessies) en las de bestaande documentatie. Hoofdstuk 1 behandelt ook de radio-eisen die voor wifi-producten al gelden (gedelegeerde verordening (EU) 2022/30) en de vraag in welke klasse het product valt. Hieronder twee punten uit het gapregister.

Er is geen procedure om een actief misbruikte kwetsbaarheid binnen 24 uur te melden

Hoog | Wie: CTO | Tijd: 2 dagen voor procedure en oefening

Wat ik zag. Kwetsbaarheden worden opgevolgd in de gewone ticketlijst. Niemand weet wie beslist dat iets "actief misbruikt" is, en het centrale meldplatform (Single Reporting Platform van ENISA) was onbekend.

Waarom het telt. Sinds 11 september 2026 moet een fabrikant een actief misbruikte kwetsbaarheid in zijn product melden via het centrale meldplatform, aan de CSIRT-coördinator van het land van zijn hoofdvestiging en tegelijk aan ENISA; dat geldt ook voor producten die al eerder verkocht zijn: een vroegtijdige waarschuwing binnen 24 uur nadat hij er kennis van kreeg, een melding binnen 72 uur en een eindverslag uiterlijk 14 dagen nadat een corrigerende of mitigerende maatregel beschikbaar is. Voor een ernstig incident gelden dezelfde 24 en 72 uur, met een eindverslag binnen een maand na de incidentmelding.

Wat te doen. Een procedure van twee pagina's: criteria voor "actief misbruikt" en "ernstig incident", de beslisser en een vervanger, het meldkanaal en een sjabloon voor de drie meldingen. Hoofdstuk 3 van het rapport bevat het ontwerp. Daarna een oefening met een verzonnen kwetsbaarheid.

Bron. Verordening (EU) 2024/2847 (Cyber Resilience Act), art. 14 (meldplicht van fabrikanten), van toepassing sinds 11 september 2026 (art. 71), ook voor producten die voor 11 december 2027 op de markt kwamen (art. 69, lid 3). Gelezen op 20 oktober 2026.

Iemand van buiten kan een kwetsbaarheid nergens melden

Hoog Wie: CTO, met de websitebouwer | Tijd: een halve dag

Wat ik zag. De website en de app vermelden alleen een algemeen contactformulier. Er is geen security.txt, geen beleid voor gecoördineerde openbaarmaking en geen vast adres voor meldingen over de beveiliging van het product.

Waarom het telt. Een onderzoeker die een fout vindt, weet niet waar hij terecht kan en publiceert ze misschien zonder u te verwittigen. Vanaf 11 december 2027 vragen de essentiële eisen een beleid voor gecoördineerde openbaarmaking en een contactadres om kwetsbaarheden te melden; ook de gebruikersinformatie moet dan dat meldpunt vermelden.

Wat te doen. Een vast adres (bijvoorbeeld security@vdhsensor.example), een security.txt op de website en een korte beleidstekst over hoe u meldingen behandelt en wanneer u publiceert. Het rapport bevat een ontwerp van die tekst.

Bron. Verordening (EU) 2024/2847, bijlage I, deel II (vereisten inzake de behandeling van kwetsbaarheden), punten 5 en 6; van toepassing vanaf 11 december 2027 (art. 71). Gelezen op 20 oktober 2026.