CVD

Coordinated Vulnerability Disclosure

welbions
Thuis in Borne en Hengelo

Februari 2024

CVD (Coordinated Vulnerability Disclosure) Kwetsbaarheid melden

Veiligheid van onze informatiesystemen (internet en bijbehorende hardware en software) zijn voor ons erg belangrijk. Ondanks onze zorg voor de beveiliging van onze systemen kan het voorkomen dat er toch een zwakke plek is.

Zwakke punten zijn op twee manieren ontdekken. Door per ongeluk iets tegen te komen tijdens normaal gebruik van onze systemen, of door echt op zoek te gaan naar zwakke plekken. Ons Responsible Disclosure-beleid is geen uitnodiging om actief ons bedrijfsnetwerk te scannen om zwakke punten te ontdekken. Dat doen we zelf al. Actieve netwerkmonitoring is aanwezig waardoor de kans groot is dat een scan wordt gedetecteerd. Dit leidt tot acties, onderzoek en onnodige kosten. Geld dat we liever besteden aan onze huurders en woningzoekenden.

Heeft u zo'n zwakke plek in één van onze systemen gevonden? Dan vragen wij u dit aan ons te melden, zodat wij snel gepaste maatregelen kunnen treffen. Wij willen graag met u samenwerken om onze huurders, medewerkers en onze systemen beter te kunnen beschermen.

Wij vragen u:

- Uw bevindingen te mailen naar privacy@welbions.nl.
- De melding zo snel mogelijk na het ontdekken van de zwakke plek bij ons te doen.
- De kwetsbaarheid niet met anderen te delen totdat deze is verholpen en alle informatie die verkregen is via het lek direct na het verhelpen van het lek te wissen.
- Ons voldoende informatie te geven om het probleem te kunnen vinden zodat wij het zo snel mogelijk kunnen verhelpen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid voldoende, maar bij complexere kwetsbaarheden kan meer nodig zijn.
- De kwetsbaarheid niet te misbruiken door bijvoorbeeld meer informatie te downloaden dan nodig is om het lek aan te tonen.
- Geen gebruik te maken van aanvallen op fysieke beveiliging, social engineering, DDoS, spam of applicaties van derden.

De volgende handelingen zijn niet toegestaan:

- Het op wat voor wijze dan ook misbruik maken van de kwetsbaarheid.
- Het plaatsen van malware, noch op onze systemen noch op die van anderen.
- Het zogeheten "bruteforcen" van toegang tot systemen.
- Het gebruik maken van social engineering.
- Het openbaar maken of aan derden verstrekken van informatie over het beveiligingsprobleem voordat het probleem is opgelost.
- Het gebruik maken van technieken waarmee de beschikbaarheid en/of bruikbaarheid van het systeem of services wordt verminderd (DoS-aanvallen).

Wij beloven dat:

- U binnen 5 werkdagen van ons een reactie krijgt.
- Wij u op de hoogte houden van de voortgang van het verhelpen van de kwetsbaarheid.
- Als u de kwetsbaarheid netjes gemeld hebt en via de bovenstaande stappen gehandeld hebt, wij geen juridische stappen zetten*,
- Wij uw melding vertrouwelijk behandelen en dat uw persoonlijke gegevens niet zonder uw toestemming met anderen delen worden tenzij dit een wettelijke verplicht is.
- Als u de kwetsbaarheid gemeld hebt volgens bovenstaande stappen, we u een beloning kunnen geven voor uw onderzoek. We zijn daartoe echter niet verplicht. U hebt dus niet zonder meer recht op een vergoeding. De vorm van deze beloning staat niet van tevoren vast en zal door ons per geval worden bepaald. Of we een beloning geven en wat voor vorm de beloning heeft, hangt af van de zorgvuldigheid van uw onderzoek, de kwaliteit van de melding en de ernst van het lek.
- In berichtgeving over het gemelde probleem we, als u dit wilt, uw naam zullen vermelden als de ontdekker. Wij streven ernaar om alle problemen zo snel mogelijk op te lossen.

Let op: ons beleid voor responsible disclosure is geen uitnodiging om ons netwerk uitgebreid te scannen om zwakke plekken te ontdekken. Er bestaat een kans dat u tijdens jouw onderzoek handelingen uitvoert die strafbaar zijn. Het feit dat Welbions geen aangifte tegen u zal doen sluit niet uit dat er een strafrechtelijk onderzoek naar uw handelen gehouden kan worden dan wel dat u strafrechtelijk kunt worden veroordeeld.