

Coordinated Vulnerability Disclosure (CVD)

De veiligheid van onze systemen heeft hoge prioriteit. Heeft u een mogelijke kwetsbaarheid gevonden? Meld deze dan zorgvuldig en vertrouwelijk. Met deze afspraken kunnen wij de melding snel onderzoeken en onze klanten, gebruikers en systemen beschermen.

Scope

Dit beleid geldt voor publiek bereikbare domeinen, websites, webapplicaties, API's en infrastructuur die aantoonbaar eigendom zijn van of worden beheerd door Condor B.V. Onderzoek is alleen toegestaan op het concrete systeem waarop de mogelijke kwetsbaarheid is aangetroffen.

Buiten scope zijn systemen van klanten en andere derden, klantomgevingen, gegevens van klanten of gebruikers, fysieke beveiliging, social engineering, phishing, spam, denial-of-serviceaanvallen, grootschalig geautomatiseerd scannen en elke test die de beschikbaarheid of integriteit van een dienst kan beïnvloeden. Vraag vooraf schriftelijke toestemming als het eigendom of de scope niet duidelijk is.

Voorwaarden voor onderzoek en safe harbour

Condor zal geen civielrechtelijke of strafrechtelijke stappen tegen u initiëren voor onderzoek dat te goeder trouw en volledig volgens deze voorwaarden wordt uitgevoerd:

- Beperk het onderzoek tot wat strikt noodzakelijk is om de kwetsbaarheid vast te stellen en aan te tonen.
- Gebruik de kwetsbaarheid niet voor financieel gewin, blijvende toegang, verstoring of verdere verspreiding.
- Bekijk, kopieer, wijzig of verwijder geen gegevens van anderen. Stop direct als u onverwacht toegang krijgt tot persoonsgegevens, vertrouwelijke informatie of systemen buiten de scope.
- Plaats geen malware, maak geen accounts aan buiten wat voor de test noodzakelijk is en pas geen wachtwoorden of configuraties aan.

- Deel de kwetsbaarheid niet met anderen en publiceer niets voordat schriftelijke afspraken over gecoördineerde publicatie zijn gemaakt.
- Lever op ons verzoek redelijke aanvullende informatie voor verificatie, zonder het onderzoek uit te breiden.

Deze safe harbour geldt vanaf het begin van het onderzoek; een overeenkomst achteraf is niet vereist. De bescherming geldt niet voor handelingen buiten deze voorwaarden, opzettelijke schade, afpersing, misbruik van gegevens of onderzoek op systemen van derden. Dit beleid geeft geen toestemming namens derden en beperkt wettelijke verplichtingen van Condor of bevoegde autoriteiten niet.

Veilig melden

Stuur eerst een korte melding zonder gevoelige bewijsstukken naar info@condor.nl met als onderwerp **CVD-melding**. Vraag in die e-mail om instructies voor beveiligde overdracht. Wij verstrekken vervolgens een beveiligde methode voor het aanleveren van technische details en bewijsstukken. Stuur geen wachtwoorden, persoonsgegevens, klantgegevens, exploits of omvangrijke logbestanden onbeveiligd per e-mail.

Neem minimaal op:

- het getroffen domein, de URL, API of het IP-adres;
- een duidelijke beschrijving, mogelijke impact en reproduceerbare stappen;
- datum en tijd van de waarneming en, indien relevant, beperkte technische bewijsstukken;
- uw contactgegevens of de vermelding dat u anoniem wilt blijven;
- uw voorkeur voor naamsvermelding bij eventuele publicatie.

Behandeling en termijnen

Stap	Streeftermijn
Ontvangstbevestiging	Binnen 1 werkdag
Eerste triage en beoordeling van scope en ernst	Binnen 3 werkdagen
Terugkoppeling over aanpak en verwachte hersteldatum	Binnen 5 werkdagen
Kritieke kwetsbaarheid	Directe beheersmaatregel; herstel met hoogste prioriteit

Stap	Streeftermijn
Hoge kwetsbaarheid	Streefdatum voor herstel binnen 14 kalenderdagen
Middelmatige kwetsbaarheid	Streefdatum voor herstel binnen 30 kalenderdagen
Lage kwetsbaarheid	Streefdatum voor herstel binnen 90 kalenderdagen of een geplande release

De ernst wordt beoordeeld met de actuele versie van CVSS, aangevuld met exploitbaarheid, blootstelling, gegevensgevoeligheid en bedrijfsimpact. Als een termijn niet haalbaar is, delen wij de reden, tijdelijke beheersmaatregelen en een nieuwe streefdatum. Wij houden de melder bij wezenlijke wijzigingen op de hoogte.

Persoonsgegevens, bewijs en bewaartermijnen

- Verzamel en deel zo min mogelijk persoonsgegevens. Maskeer gegevens die niet nodig zijn om de kwetsbaarheid aan te tonen.
- Wij gebruiken meldingen en bewijsstukken uitsluitend voor triage, onderzoek, herstel, verantwoording en eventuele wettelijke verplichtingen.
- Toegang is beperkt tot medewerkers en ingeschakelde deskundigen die de informatie nodig hebben en aan vertrouwelijkheid zijn gebonden.
- Bewijsstukken worden beveiligd opgeslagen. Niet-noodzakelijke kopieën worden na afronding verwijderd.
- Het meldingsdossier wordt niet langer bewaard dan noodzakelijk voor afhandeling en verantwoording en daarna verwijderd of geanonimiseerd volgens de geldende bewaartermijnen en het privacybeleid.
- Een vermoeden van een datalek wordt behandeld volgens het incident- en datalekproces.

Gecoördineerde publicatie en erkenning

Publicatie vindt alleen plaats na onderlinge afstemming. Uitgangspunt is publicatie nadat een oplossing of effectieve beheersmaatregel beschikbaar is. Als herstel meer tijd vraagt, spreken wij een passende publicatiedatum af op basis van het risico voor gebruikers en klanten. Wij vermelden de naam van de melder alleen met diens toestemming.

Een eventuele beloning is afhankelijk van onder meer de ernst, kwaliteit en nieuwheid van de melding. Er bestaat geen automatisch recht op een beloning.

Gerelateerde beleidsdocumenten

- Informatiebeveiligingsbeleid
- Privacybeleid
- Pentestbeleid — scoring en behandeling moeten aansluiten op de actuele versie van CVSS, waaronder CVSS 4.0.