

Beleid voor de gecoördineerde bekendmaking van kwetsbaarheden

Bij B&F Optics vinden wij de veiligheid van onze systemen en gegevens erg belangrijk. Ondanks onze zorg voor de beveiliging daarvan kan een kwetsbaarheid toch voorkomen. Als u in een van onze systemen per toeval een zwakke plek vindt, horen wij dat graag zodat wij zo snel mogelijk maatregelen kunnen treffen. Wij willen graag met u samenwerken om onze systemen, gegevens en gebruikers beter te beschermen.

Op deze pagina vindt u

- het **aanspreekpunt** aan wie u kwetsbaarheden kunt melden
- de **procedure** die wij samen met u volgen om een melding af te handelen
- welke **afspraken** u dient na te leven
- wat wij **beloven** als reactie op uw melding
- het **toepassingsgebied en toepasselijk recht** van ons beleid

1 Aanspreekpunt

Mail uw bevindingen en contactinformatie uitsluitend naar ApolloSecurity@ocuco.com

2 Procedure

2.1 Melding

- Meld uw bevindingen **zo snel mogelijk en enkel** aan het bovengenoemde aanspreekpunt.
- Geef **voldoende informatie** over het probleem zodat wij het kunnen reproduceren en zo snel mogelijk oplossen. Meestal is het IP-adres of de URL (het internetadres) van de getroffen systemen en een omschrijving van de kwetsbaarheid voldoende, maar bij complexere beveiligingsproblemen kan meer nodig zijn.

2.2 Communicatie

- Wij reageren binnen 5 werkdagen op uw melding met onze beoordeling van de melding en een verwachte datum voor een oplossing.
- Wij **informer**en u op het juiste moment over de voortgang van de oplossing van het probleem.

2.3 Onderzoek

- In deze fase controleren wij uw melding door de kwetsbaarheid te **reproduceren**.
- Wij **beoordelen** hierin ook nauwkeurig de **ernst** van het gemelde beveiligingsprobleem.

2.4 Oplossing

Het doel van ons beleid van gecoördineerde bekendmaking van kwetsbaarheden is oplossingen uit te werken vooraleer er schade berokkend kan worden. Wij zullen het probleem dan ook **zo snel mogelijk** oplossen, **in functie van de risico's** verbonden aan de kwetsbaarheid.

3 Afspraken

3.1 Uw onderzoek

Wij vragen u

- het beveiligingsprobleem niet te misbruiken door méér data te downloaden, te kopiëren, in te kijken, te verwijderen, aan te passen of beschikbaar te stellen dan nodig is om het lek aan te tonen
- vertrouwelijke gegevens die u via de kwetsbaarheid gevonden heeft, niet met anderen te delen en ze onmiddellijk te wissen nadat wij het beveiligingsprobleem opgelost hebben.
- Geen gebruik te maken van aanvallen op fysieke beveiliging, social engineering, distributed denial of service, spam of applicaties van derden, geen malware te plaatsen (virussen, wormen, Trojaanse paarden enz.)
- geen veranderingen in het systeem aan te brengen
- de vertrouwelijkheid, de integriteit, de beschikbaarheid en het prestatievermogen van onze systemen niet aan te tasten.

Het is mogelijk dat u tijdens uw onderzoek kennisneemt van vertrouwelijke gegevens. Dat begrijpen we. Die kennisneming mag echter niet het opzet van uw onderzoek zijn, maar mag enkel toevallig gebeuren bij het opsporen van beveiligingsproblemen.

3.2 Uw publicatie

Als u het bestaan van een beveiligingsprobleem met derden wenst te delen, vragen wij u

- dat enkel te doen nadat wij het hebben opgelost
- ons daar een maand op voorhand van te verwittigen om ons de kans te geven te reageren
- ons toe te laten in overleg met u te beslissen hoe het bestaan van het probleem gedeeld wordt
- B&F Optics noch een van haar merken rechtstreeks of onrechtstreeks in uw publicatie te identificeren zonder ons uitdrukkelijk akkoord.

4 Wat wij beloven

- Wij reageren binnen vijf werkdagen op uw melding.
- Wij informeren u over de voortgang van het oplossen van het probleem.
- Wij proberen het probleem zo snel mogelijk op te lossen.
- Als u zich aan de bovenstaande afspraken houdt, zullen wij geen juridische stappen tegen u ondernemen.
- Wij behandelen uw melding vertrouwelijk en zullen uw persoonlijke gegevens niet zonder uw toestemming met derden delen tenzij dat noodzakelijk is om een wettelijke verplichting na te komen.
- In berichtgeving over het gemelde probleem zullen wij, indien u dit wenst, uw naam vermelden als de ontdekker, en
- Als dank voor uw hulp bieden wij een beloning aan voor elke melding van een ons nog onbekend beveiligingsprobleem. De grootte van de beloning bepalen wij aan de hand van de ernst van het lek en de kwaliteit van de melding met een minimum van een bol.com waardebon van €50,-.

5 Toepassingsgebied en toepasselijk recht

Als er een geschil tussen ons zou ontstaan over de toepassing, naleving of interpretatie van dit beleid, en we kunnen dat niet minnelijk regelen, zal het aan de bevoegde rechtbank in 's-Hertogenbosch voorgelegd worden. Het Nederlands recht is toepasselijk.