Coordinated Vulnerability Disclosure

Datum laatste wijziging	06/11/2024
Auteurs	CISO
Documenttype	Responsible Disclosure beleid
Classificatie	Publiek
Distributie	Nvt
Versie	1.0
Eigenaar	CISO
Status	Definitief

Insign.it bv
Noorderpoort 69, 5916 PJ Venlo
Postbus 213, 5900 AE Venlo

+31 77 472 00 15
insign.it
info@insign.it

K.v.K. Venlo 12042097
BTW nummer NL808911375B01

IBAN NL89RABO0128088796
BIC RABONL2U

insign.it

Inhoudsopgave

1 Welkom

We waarderen jouw inzet om onze systemen veiliger te maken! Als je een beveiligingskwetsbaarheid hebt gevonden in een van onze systemen of applicaties, horen we dat graag van je. Dit beleid legt uit hoe je dat kunt doen en wat je van ons kunt verwachten.

2 Wat we vragen

Als je denkt dat je een kwetsbaarheid hebt ontdekt, willen we je vragen om:

- **Meld het aan ons:** Stuur ons een e-mail naar servicedesk@insign.it met een beschrijving van wat je hebt gevonden. U kunt bij ons kwetsbaarheden melden die een risico vormen voor de beveiliging van een systeem. Voorbeelden hiervan zijn kwetsbaarheden die het mogelijk maken om een login-formulier te omzeilen of op een onbedoelde manier toegang te krijgen tot een database met persoonsgegevens.
- **Wees duidelijk:** Geef ons zoveel mogelijk details. Hoe heb je het probleem gevonden? Welke stappen hebben je ertoe gebracht?
- **Testen:** Geen tests uit te voeren die gebruik maken van aanvallen op fysieke beveiliging, DDOS, social engineering of applicaties van derden.
- **Geen bijlages sturen:** Gebruik geen bijlages of hyperlinks in je mail, maar verwerk jouw stappen in de mail.
- **Openbaar:** Het probleem niet openbaar te maken voordat wij een oplossing hebben geïmplementeerd.
- **Gegevens:** Geen gegevens van onze gebruikers te manipuleren of te verwijderen.
- **Onderzoek:** De kwetsbaarheid niet verder te onderzoeken dan nodig is om uw bevindingen aan ons te rapporteren.
- **Respecteer privacy:** Probeer geen gegevens van anderen in te zien, te wijzigen, of te verwijderen.

3 Wat kun je niet melden

- Ons beleid ten aanzien van de aanwezigheid of afwezigheid van SPF/DKIM//DANE/DNSSEC/DMARC.
- Mogelijk verouderde server- of applicatieversies (van externe partijen) zonder bewijs dat deze versies kwetsbaar zijn en zonder bewijs van exploitatie.
- Generieke kwetsbaarheden gerelateerd aan software of protocollen die niet onder controle van Insign.it vallen.
- Rapporten van reguliere scans zoals poortscanners.

4 Wat je van ons kunt verwachten

Als je ons een melding stuurt, zullen we:

- **Snel reageren:** We laten je binnen 3 werkdagen weten dat we je melding hebben ontvangen.
- **Onderzoek doen:** We nemen de tijd om te onderzoeken wat je hebt gevonden en geven je updates over onze voortgang.
- **Problemen oplossen:** Als er inderdaad een probleem is, zullen we werken aan een oplossing en je laten weten wanneer het is opgelost.

5 Geen boze gezichten

We weten dat je het beste met ons voor hebt, dus we zullen geen juridische stappen ondernemen als je ons op een vriendelijke en respectvolle manier helpt om problemen te ontdekken en op te lossen.

6 Wijzigingen in dit beleid

We behouden ons het recht voor om dit beleid op elk moment te wijzigen.

insign.it

7 Bedankje

Als je ons helpt een serieus probleem op te lossen, willen we je graag bedanken. Dat kan variëren van een publieke vermelding op onze website tot een leuke beloning van minimaal 50,-.