HZ Responsible Disclosure Statement

Bij HZ University of Applied Sciences vinden wij de veiligheid van onze systemen erg belangrijk. Ondanks de zorg die we besteden aan de beveiliging van onze systemen kan het voorkomen dat er toch een zwakke plek is.

Als u een zwakke plek in één van onze systemen of procedures heeft gevonden, dan horen wij dit graag zodat we zo snel mogelijk maatregelen kunnen treffen. HZ wil graag met u op de hieronder beschreven manier samenwerken om onze gebruikers en onze systemen beter te kunnen beschermen.

Wij vragen u:

- Uw bevindingen te mailen naar security@HZeeland.nl. Versleutel uw bevindingen met onze PGP key (fingerprint: 7D55 B928 638A CF17 6A41 2477 A0F6 67BC DC89 9C3F) om te voorkomen dat de informatie in verkeerde handen valt.

- Het gevonden probleem niet te misbruiken door bijvoorbeeld meer data te downloaden dan nodig is om het lek aan te tonen of door het veranderen of verwijderen van gegevens en extra terughoudendheid te betrachten bij persoonsgegevens.

- Het probleem niet met anderen te delen totdat het is opgelost en alle vertrouwelijke gegevens die zijn verkregen via het lek direct na het dichten ervan te wissen.

- Geen gebruik te maken van aanvallen op fysieke beveiliging of applicaties van derden, van social engineering, distributed denial-of-service, of spam.

- Voldoende informatie te geven om het probleem te reproduceren zodat wij het zo snel mogelijk kunnen oplossen. Meestal is het IP-adres of de URL van het getroffen systeem, een omschrijving van de kwetsbaarheid en de uitgevoerde handelingen voldoende, maar bij complexere kwetsbaarheden kan aanvullende informatie nodig zijn.

Wat HZ belooft:

- Vanuit HZ wordt binnen 3 werkdagen op uw melding gereageerd met onze beoordeling van de melding en een verwachte datum voor een oplossing.

- 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.

- Wij houden u op de hoogte van de voortgang van het oplossen van de kwetsbaarheid.

- Anoniem of onder een pseudoniem melden is mogelijk. Het is voor u goed om te weten dat dit wel betekent dat wij dan geen contact kunnen opnemen over bijvoorbeeld de vervolgstappen, voortgang van het dichten van het lek of publicatie.

- In berichtgeving over de gemelde kwetsbaarheid zullen wij, indien u dit wenst, uw naam vermelden als de ontdekker van de kwetsbaarheid.

- Als dank voor uw onderzoek en melding kan HZ besluiten kleine attentie te sturen. Of uw melding hiertoe aanleiding geeft, zal per incident worden beoordeeld. Hierbij moet opgemerkt dat HZ onder geen enkele voorwaarde een financiële vergoeding uitkeert.

Wij streven ernaar om alle problemen zo snel mogelijk op te lossen, de betrokken partijen op de hoogte te houden en blijven we graag betrokken bij een eventuele publicatie over de vastgestelde kwetsbaarheid nadat het is opgelost.

Aanvullend:

HZ University of Applied Sciences neemt geen meldingen van triviale kwetsbaarheden in behandeling, of van bugs die niet misbruikt kunnen worden. De volgende, niet limitatieve, lijst van bekende en aanvaardbare risico's valt niet binnen de reikwijdte van onze responsible disclosure policy en zullen niet in behandeling worden genomen wanneer aangemeld via security@HZeeland.nl:

- HTTP 404 codes/pages or other HTTP non-200 codes/pages and Content Spoofing/Text Injection on these pages;
- fingerprint version banner disclosure on common/public services;
- disclosure of known public files or directories or non-sensitive information, (e.g. robots.txt);
- clickjacking and issues only exploitable through clickjacking;
- lack of Secure/HTTPOnly flags on non-sensitive Cookies;
- OPTIONS HTTP method enabled;
- anything related to HTTP security headers, e.g.:
    - Strict-Transport-Security;
    - X-Frame-Options;
    - X-XSS-Protection;
    - X-Content-Type-Options;
    - Content-Security-Policy.
- SSL Configuration Issues:
    - SSL forward secrecy not enabled;
    - weak / insecure cipher suites.
- SPF, DKIM, DMARC issues;
- host header injection;
- reporting older versions of any software without proof of concept or working exploit;
- information leakage in metadata;
- Systems and protocols that can be used in DDoS attacks;
- Intentional listing of directory contents for research or publication purposes;
- Missing DNSSEC configuration.