Over Responsible Disclosure

Weerbare Digitale Overheid hecht veel belang aan de beveiliging van haar systemen. Ondanks alle voorzorgsmaatregelen blijft het mogelijk dat een zwakke plek in de systemen te vinden is. Wanneer u een zwakke plek in één van onze systemen ontdekt, vernemen wij dit graag van u, zodat wij snel gepaste maatregelen kunnen nemen. Door het maken van een melding zal Weerbare Digitale Overheid uw melding conform onderstaande afspraken afhandelen.

Wij vragen het volgende van u:

- Mail uw bevindingen naar **registratie@spitz.nu**. Versleutel de bevindingen indienmogelijk met onze PGP-sleutel om te voorkomen dat de informatie in verkeerde handen valt.
- Geef voldoende informatie om het probleem te reproduceren, zodat we het zo snel mogelijk kunnen oplossen. 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.
- Wij houden ons aanbevolen voor tips die ons helpen het probleem op te lossen. Beperkt u zich daarbij wel graag tot verifieerbare feitelijkheden die betrekking hebben op de door u geconstateerde kwetsbaarheid en vermijd dat uw advies in feite neerkomt op reclame voor specifieke (beveiligings-)producten.
- Contactgegevens achter te laten zodat we met u in contact kunnen treden om samen te werken aan een veilig resultaat. Laat minimaal één e-mailadres of telefoonnummer achter.
- Dien de melding a.u.b. zo snel mogelijk in na ontdekking van de kwetsbaarheid.

De volgende handelingen zijn niet toegestaan

- Het plaatsen van malware, noch op onze systemen noch op die van anderen;
- Het zogeheten “bruteforcen” van toegang tot systemen, behalve voor zover dat strikt noodzakelijk is om aan te tonen dat de beveiliging op dit vlak ernstig tekort schiet, dat wil zeggen als het buitengewoon eenvoudig is om met openbaar verkrijgbare en goed betaalbare hardware en software een wachtwoord te kraken waarmee het systeem ernstig kan worden gecompromitteerd;
- Het gebruik maken van social engineering, behalve voor zover dat strikt noodzakelijk is om aan te tonen dat medewerkers met toegang tot gevoelige gegevens in het algemeen (ernstig) tekort schieten in hun plicht om daar zorgvuldig mee om te gaan. Dat wil zeggen als het op overigens volkomen legale wijze (dus niet via chantage of iets dergelijks) in het algemeen te eenvoudig is om hen over te halen tot het verstrekken van dergelijke gegevens aan onbevoegden. U dient daarbij alle zorg te betrachten die redelijkerwijs van u verwacht kan worden om de betreffende medewerkers zelf niet te schaden. Uw bevindingen dienen uitsluitend te zijn gericht op het aantonen van kennelijke gebreken in de procedures en werkwijze binnen Weerbare Digitale Overheid en niet op het schaden van individuele personen die bij Weerbare Digitale Overheid werkzaam zijn;
- Het openbaar maken of aan derden verstrekken van informatie over het beveiligingsprobleem voordat het is opgelost;
- Het verrichten van handelingen die verder gaan dan wat strikt noodzakelijk is om het beveiligingsprobleem aan te tonen en te melden. In het bijzonder waar het gaat om het verwerken (waaronder het inzien of kopiëren) van vertrouwelijke gegevens waar u door de kwetsbaarheid toegang toe heeft gehad. In plaats van een complete database te kopiëren, kunt u normaliter volstaan met bijvoorbeeld een directory listing. Het wijzigen of verwijderen van gegevens in het systeem is nooit toegestaan;
- Het gebruik maken van technieken waarmee de beschikbaarheid en/of bruikbaarheid van het systeem of services wordt verminderd (DoS-aanvallen);
- Het op wat voor (andere) wijze dan ook misbruik maken van de kwetsbaarheid.

Wat wij beloven

- Indien u aan alle bovenstaande voorwaarden voldoet, zullen wij geen strafrechtelijke aangifte tegen u doen en ook geen civielrechtelijke zaak tegen u aanspannen.
- Als blijkt dat u een bovenstaande voorwaarde toch heeft geschonden, kunnen wij alsnog besluiten om gerechtelijke stappen tegen u te ondernemen.

- Wij behandelen een melding vertrouwelijk en delen persoonlijke gegevens van een melder niet zonder diens toestemming met derden, tenzij wij daar volgens de wet of een rechterlijke uitspraak toe verplicht zijn.
- In onderling overleg kunnen we, indien u dit wenst, uw naam vermelden als de ontdekker van de gemelde kwetsbaarheid. In alle andere gevallen blijft u anoniem.
- Wij sturen u binnen 1 werkdag een (automatische) ontvangstbevestiging en wij houden u op de hoogte van de voortgang van de oplossing.