

RESPONSIBLE DISCLOSURE

RESPONSIBLE DISCLOSURE BIT B.V. – VERSIE 2018-04-12

Bij BIT vinden wij de veiligheid van onze systemen erg belangrijk. Ondanks de uiterste zorg die wij besteden aan de beveiliging hiervan kan het voorkomen dat er toch een zwakke plek is. Als u een zwakke plek in één van onze systemen aantreft horen wij dit uiteraard graag zodat we zo spoedig mogelijk maatregelen kunnen treffen. Wij willen graag met u samenwerken om zowel onze klanten als onze systemen beter te beschermen.

De infrastructuur van BIT wordt ook door systemen van derden gebruikt en in veel gevallen ook door die derden beheerd. Zwakke plekken in systemen die door derden beheerd worden, vallen niet onder dit responsible disclosure beleid. Systemen waarvoor dit beleid in ieder geval niet geldt hebben een hostname die vm.bit.nl, colo.bit.nl of customer.bit.nl bevat. U kunt desalniettemin meldingen plaatsen voor systemen met dergelijke hostnames. U gaat er daarbij vooraf mee akkoord dat uw melding ongecensureerd wordt doorgezet naar de beheerder van het betreffende systeem. In dergelijke gevallen vervallen de beloftes van BIT zoals hieronder beschreven.

Wij vragen u:

- Geen gebruik te maken van aanvallen op fysieke beveiliging, social engineering, distributed denial of service, spam of geautomatiseerde tools, zoals vulnerability scanners.
- Het probleem niet te misbruiken door bijvoorbeeld meer data te downloaden dan nodig is om het lek aan te tonen of gegevens van derden in te kijken, te verwijderen of aan te passen.
- Het probleem niet met anderen te delen totdat het is opgelost.
- Uw bevindingen te mailen naar cert@bit.nl. Versleutel uw bevindingen met onze PGP key (ID 9DCA4A97A80E77B1) om te voorkomen dat de informatie in verkeerde handen valt.
- 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 en een omschrijving van de kwetsbaarheid voldoende, maar bij complexere kwetsbaarheden kan meer nodig zijn.
- Alle gegevens die zijn verkregen via het lek, te wissen.

Wat wij beloven:

- Als u zich aan bovenstaande voorwaarden heeft gehouden zullen wij geen juridische stappen tegen u ondernemen betreffende de melding.
- Wij reageren binnen 3 werkdagen op uw melding met onze beoordeling en een datum wanneer wij verwachten een oplossing te hebben.
- Wij houden u op de hoogte van de voortgang van het oplossen van het probleem.
- Wij behandelen uw melding vertrouwelijk en zullen uw persoonlijke gegevens niet zonder uw toestemming met derden delen tenzij dit noodzakelijk is om een wettelijke verplichting na te komen.
- Melden onder een pseudoniem is mogelijk.
- In berichtgevingen over het gemelde probleem zullen wij, indien u dit wenst, uw naam vermelden als de ontdekker.
- Als dank voor uw hulp bieden wij een beloning aan voor elke melding van een ons nog onbekend beveiligingsprobleem die daadwerkelijk een risico vormt voor ons of voor onze klanten. De grootte van de beloning bepalen wij aan de hand van de ernst van het lek en de kwaliteit van de melding. Dit met een minimum van een waardebon van € 50,-.

Wij streven er naar om alle problemen zo snel mogelijk op te lossen en worden graag betrokken bij een eventuele publicatie over het probleem nadat deze is opgelost.

De bovenstaande tekst is gebaseerd op het werk van Floor Terra zoals het gepubliceerd is op <https://www.responsibledisclosure.nl>.

De aangepaste tekst is gepubliceerd onder de Creative Commons Naamsvermelding 3.0 licentie.