webmethod_

Responsible Disclosure beleid

De ingangsdatum voor de geldigheid van deze voorwaarden is 29/08/2019.

Bij Webmethod vinden we de veiligheid van onze systemen, ons netwerk, onze producten en onze overige diensten erg belangrijk. We besteden hier veel aandacht aan bij de ontwikkeling en onderhoud. Natuurlijk kan het desondanks voorkomen dat een zwakke plek wordt ontdekt. Het is fijn als u dat aan ons laat weten. Bij voorkeur horen we dit graag zo snel mogelijk, zodat we maatregelen kunnen treffen om onze klanten te beschermen.

Dit document beschrijft de procedure die we hiervoor hebben opgesteld.

Melding doen

Verstuur de melding liefst zo snel mogelijk na ontdekking van de kwetsbaarheid aan security-external@webmethod.nl. U kunt op dit e-mailadres ook onze PGP sleutel opvragen.

Spelregels

- Deel informatie over het beveiligingsprobleem niet met anderen totdat het probleem is opgelost.
- Geef informatie over hoe en wanneer de kwetsbaarheid of storing zich voordoet. Beschrijf duidelijk hoe dit probleem gereproduceerd kan worden en geef informatie over de gebruikte methode en het tijdstip van onderzoeken.
- Ga verantwoordelijk om met de kennis over het beveiligingsprobleem. Verricht geen handelingen die verder gaan dan wat nodig is om het beveiligingsprobleem aan te tonen. Maak geen misbruik van de zwakke plek en bewaar geen vertrouwelijke gegevens die zijn verkregen via de kwetsbaarheid in het systeem.
- Laat desgewenst contactgegevens (e-mailadres of telefoonnummer) achter zodat Webmethod contact met u kan opnemen over de beoordeling en voortgang van de oplossing van de kwetsbaarheid. We nemen anonieme meldingen eveneens serieus.
- Maak geen gebruik van fysieke aanvallen, DDOS aanvallen of social engineering.

Ons responsible disclosure-beleid is geen uitnodiging om ons bedrijfsnetwerk uitgebreid actief te scannen op zwakke plekken. Wij monitoren ons netwerk zelf. Hierdoor is de kans groot dat een scan wordt opgepikt en ons team hier onderzoek naar gaat doen.

Wat doet Webmethod bij Responsible Disclosure?

Wanneer u melding doet van een vermoede zwakke plek in een ICT-systeem, dan behandelen we deze op de volgende manier:

- U krijgt binnen drie werkdagen na het doen van de melding een ontvangstbevestiging van Webmethod.
- Binnen drie werkdagen na de ontvangstbevestiging ontvangt u een reactie met daarin een beoordeling van de melding en de verwachte datum van de oplossing. We streven ernaar u ook tussentijds op de hoogte te houden over de voortgang van het oplossen van het probleem.
- Webmethod behandelt uw melding vertrouwelijk en deelt uw gegevens niet zonder uw toestemming met derden, behalve als dit wettelijk of door een rechterlijke uitspraak verplicht is.

- Webmethod zal samen met u bepalen of en hoe over het gemelde probleem wordt bericht. Berichtgeving vindt pas plaats nadat het probleem is opgelost. In de berichtgeving over het gemelde probleem zal Webmethod, indien gewenst, uw naam vermelden als ontdekker.

Wat kunt u niet melden?

Deze Responsible Disclosure regeling is niet bedoeld voor het melden van klachten. Ook is de regeling niet bedoeld voor:

- Het melden dat de website niet beschikbaar is.
- Het melden van nep e-mails (phishing e-mails).
- Het melden van fraude.

Neem voor deze en overige zaken contact op via info@webmethod.nl

UITGESLOTEN SYSTEMEN

- status.webmethod.nl
- ns{1-4}.webmethod.nl
- noc.webmethod.nl
- *.domeinen.webmethod.nl

UITGESLOTEN TYPEN BEVEILIGINGSPROBLEMEN

- (D)DOS aanvallen
- Problemen die neerkomen op self-XSS
- Foutmeldingen zonder gevoelige gegevens
- Meldingen waaruit door ons gebruikte software is af te leiden
- Problemen die gebruik van sterk verouderde besturingssystemen, browsers of incourante plugins vereisen
- Problemen die ons al bekend zijn

Dit beleid is opgesteld aan de hand van de Leidraad Responsible Disclosure van het NCSC.