Out-Of-Scope

De hieronder beschreven 'Out-of-Scope' beschrijft zaken welke wij op voorhand niet in behandeling nemen daar deze worden gezien als triviaal en niet-bedreigend.

Indien deze alsnog worden gemeld zullen wij de melder in kwestie op de hoogte brengen dat de melding out-of-scope is en zullen wij de deelnemer alsnog informeren over hetgeen er is gemeld zodat deze zelf een afweging kan maken omtrent de afhandeling.

Nederlands:

Niet in scope:

Z-CERT neemt geen triviale kwetsbaarheden of securityissues die niet misbruikt kunnen worden, in behandeling. Hieronder staan voorbeelden van bekende kwetsbaarheden en securityissues die buiten bovenstaande regeling vallen. Dit houdt niet dat ze niet opgelost zouden moeten worden, echter bij ons CVD-proces gaat het om melden van zaken waar direct misbruik van gemaakt kan worden. Bijvoorbeeld een kwetsbaarheid waar een werkende exploit voor bestaat of een misconfiguratie waardoor een bestaande securitycontrol te omzeilen is. Deze lijst is afgeleid van de lijst van die het CERT van Surf hanteert (https://www.surf.nl/responsible-disclosure-surf).

– HTTP 404 codes/pagina's of andere HTTP non-200 codes/pagina's en content spoofing/text injecting op deze pagina's
– Fingerprinting/versievermelding op publieke services
– Publieke bestanden of directories met ongevoelige informatie (bijvoorbeeld robots.txt)
– Clickjacking en problemen die alleen te exploiten zijn via clickjacking
– Geen secure/HTTP-only flags op ongevoelige cookies
– OPTIONS HTTP method ingeschakeld
– Rate limiting kwetsbaarheden zonder duidelijke impact

Alles gerelateerd tot HTTP security headers, bijvoorbeeld:
– Strict-Transport-Security
– X-Frame-Options
– X-XSS-Protection
– X-Content-Type-Options
– Content-Security-Policy

– Issues met SSL-configuratie
– SSL Forward secrecy uitgeschakeld

– Ontbrekende TXT record voor DMARC of CAA record
– Host header injection
– Rapporteren van verouderde versies van enige software zonder een proof of concept van een werkende exploit