Wat is de NCSC-NL matrix?
De beveiligingsadviezen van NCSC-NL bevatten een inschaling van de beschreven kwetsbaarheid. Per advies wordt een Kans op uitbuiting en Schade bij uitbuiting gedefinieerd. De mogelijke waarden per onderdeel zijn Low, Medium of High. Voor zowel de Kans als Schade inschalingen wordt een set vragen beantwoord, die leiden tot een waarde. Wanneer er specifieke omstandigheden zijn, kan worden afgeweken van de matrix en kan de waarde voor Kans en/of Schade worden veranderd. Kwetsbaarheden waarvan zowel de Kans als de Schade als Low wordt ingeschaald, worden niet uitgestuurd.

Kans
De kans wordt bepaald door onderstaande vragen te beantwoorden en de waarde toe te kennen die achter elke optie staat.

Vraag	Optie 1		Optie 2		Optie 3	
Is de kwetsbaarheid aanwezig in de standaard configuratie/installatie?	Nee	1	Onduidelijk/Ja	3		
Is er Exploitcode beschikbaar?	Geen	1	Proof of Concept (PoC)	4	Exploit	6
Zijn er technische details beschikbaar	Geen	1	Enigszins	2	Volledig	3
Vereiste toegang	Fysiek	1	LAN/directe omgeving	4	internet	6
Vereiste credentials?	Admin	1	User	2	Geen	4
Hoe complex is het technisch gezien om de kwetsbaarheid uit te buiten?	Complex	1	Gemiddeld	2	Eenvoudig	3
Is er gebruikersinteractie nodig?	Complex	1	Eenvoudig	3	Geen	4
Wordt de kwetsbaarheid in het wild uitgebuit?	Nee	1	Beperkt	2	Grootschalig	3
Wordt de kwetsbaarheid, naar verwachting, op korte termijn misbruikt of verschijnt er een exploit?	Nee	1	Ja	3		
Beschikbaarheid oplossing?	Ouder dan 2 maanden	1	Tot 2 maand oud	2	Geen	3

<u>Verklaring van de kans vragen:</u>

Is de kwetsbaarheid aanwezig in de standaard configuratie/installatie?:
Wanneer de kwetsbaarheid zich in een specifieke configuratie-instelling of installatie bevindt, is de kans dat een systeem kwetsbaar is minder groot dan wanneer de kwetsbaarheid standaard aanwezig is.

Is er Exploitcode beschikbaar?:

Hoe minder een aanvaller hoeft te doen om systemen te kunnen compromitteren, hoe hoger de kans dat dit ook gebeurt.

Zijn er technische details beschikbaar:
Hoe meer technische details beschikbaar zijn, hoe (relatief) eenvoudiger het wordt om een exploit te schrijven wat de kans dat deze verschijnt vergroot. Mogelijke waarden zijn:

- Geen: er zijn geen details over de kwetsbaarheid gepubliceerd.
- Enigszins: er is een aantal details gepubliceerd. Het is bekend welke component of functie een probleem bevat en onder welke omstandigheden de kwetsbaarheid aanwezig is.
- Volledig: het exacte commando binnen de kwetsbare functie bekend is gemaakt, of kwetsbaarheid is aangetoond in de broncode.

Vereiste toegang:
De kans dat een kwetsbaar systeem wordt gecompromitteerd wanneer het toegankelijk is voor een beperkte groep mensen is kleiner dan wanneer het rechtstreeks vanaf het internet benaderbaar is. Mogelijke waarden zijn:

- Fysiek/Directe omgeving: de aanvaller moet fysiek in de buurt van het systeem zijn of met een gebruikersaccount kunnen inloggen.
- LAN: De aanvaller moet via het LAN netwerkverkeer kunnen sturen naar het kwetsbare systeem.
- Internet: Diensten zoals een webserver of een mailserver zullen worden aangemerkt als benaderbaar via het internet.

Vereiste credentials:
Wat voor gebruikersrechten heeft de aanvaller nodig om de kwetsbaarheid te kunnen uitbuiten?

Hoe complex is het technisch gezien om de kwetsbaarheid uit te buiten
Een kwetsbaarheid die eenvoudig uit te buiten is zal mogelijk eerder tot een werkende exploit leiden dan een technisch zeer complex probleem.

Is er gebruikersinteractie nodig?:
Moet de gebruiker worden overgehaald om een document te openen of een website te bezoeken?

Wordt de kwetsbaarheid in het wild uitgebuit?:
Wordt actief misbruikt op het internet? Is er sprake van grootschalig misbruik? Of een gerichte aanval?

Wordt de kwetsbaarheid binnenkort misbruikt of verschijnt er een exploit?
Deze vraag kent een gevoelswaarde toe aan de inschaling.

Beschikbaarheid oplossing:
Wanneer er geen oplossing bekend is, is het zeer interessant voor aanvallers om de kwetsbaarheid uit te buiten

Door bovenstaande waarden toe te kennen aan de antwoorden ontstaat een kanswaarde per kwetsbaarheid. Op basis van discussiesessies en meerdere proefwegingen is bepaald dat de onderstaande verdeling wordt gehanteerd om een betrouwbare inschaling te doen.

- Low: 10 – 18
- Medium: 19 – 27
- High: 28 - 38

Schade

De schade wordt bepaald door een van de onderstaande schadeomschrijvingen te kiezen. Wanneer meer dan één type schade kan worden veroorzaakt, wordt de zwaarste inschaling gebruikt.

Schadeomschrijving

Denial of Service (DoS):
De kwetsbaarheid kan ertoe leiden dat een dienst niet meer bereikbaar/bruikbaar is

Uitvoeren van willekeurige code:
Na uitbuiting kan code of systeemcommando's worden uitgevoerd.

Rechten op afstand (remote (root-) shell):
Na uitbuiten van de kwetsbaarheid krijgt de aanvaller toegang tot een interactieve (root-)shell op afstand.

Verwerven lokale admin/root-rechten (privilege escalation):
Een reguliere gebruiker kan zich verhoogde rechten toe-eigenen door het uitbuiten van de kwetsbaarheid op het lokale systeem.

Lekkage informatie:
Door een kwetsbaarheid uit te buiten kan systeeminformatie of data buit worden gemaakt.

Vraag	Optie 1		Optie 2		Optie 3	
Denial of Service	Nee	Low	Ja, Client	Low	Ja, Infrastructuur dienst	High
Uitvoeren van willekeurige code	Nee	Low	Ja, Gebruikers rechten	Medium	Ja, Root / Administrator rechten	High
Rechten op afstand (remote (root-) shell)	Nee	Low	Ja, remote shell	Medium	Ja, remote root-shell	High
Verwerven lokale admin/root-rechten (privilege escallation)	Nee	Low	Ja	Medium		
Lekkage informatie	Nee	Low	Ja, systeem informatie	Medium	Ja, data	High