Tijdens het onderzoek wordt gekeken naar de normenkaders die het UWV hanteert op het gebied van security bevindingen. Specifiek voor webapplicaties wordt gekeken naar het Secure Software Development(SSD)-normenkader. UWV vereist dat omgevingen voldoen aan dit normenkader. Meer informatie over deze normen is terug te vinden op:

- Voor webapplicaties:
  https://www.cip-overheid.nl/media/clkmwp3x/20200720-ssd-normen-v30.pdf
- Voor mobiele applicaties:
  https://www.cip-overheid.nl/media/jglbccmm/20160225_grip_op_ssd_mobile_apps_beveiligingseisen_v1-00.pdf

De mate van afwijking aan het voldoen aan dit normenkader kan als factor meegenomen worden in het geven van een eventueel negatief advies voor ingebruikname. Verder volgt het UWV de NCSC richtlijnen voor webapplicaties, TLS en mobiele applicaties:

- Voor webapplicaties:
  https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties/Richtlijn_ICT+beveiligingsrichtlijnen+webapplicaties_juli24_NL.pdf
- Voor TLS:
  https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1/ICT-beveiligingsrichtlijnen+voor+Transport+Layer+Security+v2.1.pdf
- Voor mobiele applicaties:
  https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-mobiele-apps/ict-beveiligingsrichtlijnen-voor-mobiele-apps_archief.pdf

Afwijkingen hierop zullen worden gerapporteerd. Daarnaast kunnen er beveiligingsrisico's worden gevonden en gerapporteerd die niet van toepassing zijn op een norm of richtlijn.

Classificatie van bevindingen

De classificatie geeft de noodzaak aan tot het verhelpen van de bevinding. De bevindingen worden geclassificeerd als "Informatief", "Laag", "Midden" en "Hoog" risico. De beschrijving voor de classificatie is als volgt.

Hoog

De bevinding kan direct leiden tot verlies van productie-/persoonsgegevens of over de controle van het systeem. Het verlies van persoonsgegevens zal altijd leiden tot een "Hoog" bevinding.

Midden

De bevinding kan indirect leiden tot verlies van productie-/persoonsgegevens of over de controle van het systeem. Hiervoor dient de aanvaller eerst een andere kwetsbaarheid te misbruiken of heeft eerst interactie met de gebruiker nodig om tot de gegevens te komen. Let wel dat meerdere "Midden" en/of "Laag" geclassificeerde bevindingen mogelijk samen tot een "Hoog" bevinding kunnen leiden.

Laag

De bevinding levert niet direct voordeel op voor een mogelijke aanvaller. Het misbruiken van een dergelijke bevinding zal niet direct leiden tot verlies van productie-/persoonsgegevens of over de controle van het systeem. Let wel dat meerdere "Midden" en/of "Laag" geclassificeerde bevindingen mogelijk samen tot een "Midden" of "Hoog" bevinding kunnen leiden.

Informatief

De bevinding leidt niet tot verlies van productie-/persoonsgegevens of over de controle van het systeem of levert niet direct voordeel op voor een mogelijke aanvaller. De inrichting wijkt echter af van de richtlijnen die UWV volgt (bijvoorbeeld de SSD-normen) of is niet marktconform en wordt daarom wel gemeld. In het geval dat een “Informatief” bevinding gekoppeld is aan een UWV gehanteerde richtlijn (bijvoorbeeld de SSD-normen), dan zal het risico wel moeten worden verholpen of met de daarvoor bestemde processen worden verantwoord.