

STICHTING SCHULDENKNOOPPUNT

PUBLIEKE SAMENVATTING BEVEILIGINGSONDERZOEK API "PAUZE SIGNAAL" EN
"SBENSK VERSIE 3"

Datum rapport
Classificatie
Versie

19/12/2025
Openbaar
1.0

SCOPE EN DOEL

InCyber is door Schuldenknooppunt gevraagd om een penetratietest uit te voeren op de API van de nieuwe “Pauze Signaal”-module en de “SbEnSK versie 3”-module binnen de Schuldenknooppunt applicatie. Het doel van deze controle is om de beschikbaarheid, integriteit en vertrouwelijkheid van de modules te testen.

AANPAK

Het onderzoek is uitgevoerd door de API endpoints te toetsen aan onder andere de OWASP API Top 10. De API endpoints zijn op twee verschillende manieren beschikbaar, namelijk middels REST en SOAP. Een REST endpoint gebruikt standaard HTTP-operaties en stateless communicatie, waarbij elke aanvraag alle benodigde informatie bevat. Een SOAP endpoint gebruikt XML-berichten binnen een strikt gedefinieerd berichtformaat met vooraf vastgelegde berichtenstructuur. Er is vastgesteld welke risicocategorieën uit de OWASP API Top 10 relevant zijn voor de te onderzoeken API's. Op basis daarvan is een testmethodologie opgesteld waarmee de relevante risico's systematisch zijn beoordeeld per API en endpoint. Daarnaast zijn de REST endpoints volledig getest met de door ons opgestelde testmethode door de variabelen met een unieke naam te controleren en zijn de resterende risico's binnen SOAP aanvullend getest.

AANDACHTSPUNTEN

Tijdens de pentest zijn in totaal vier aandachtspunten geïdentificeerd, elk met een lage kans op exploitatie en beperkte impact bij misbruik. Deze bevindingen hebben betrekking op de striktheid van de validatie van invoervelden. Hoewel deze bevindingen naar verwachting geen direct beveiligingsrisico vormen voor de applicatie of de onderliggende systemen van klanten, kunnen zij wel leiden tot onjuiste of vervuilde data binnen het systeem.

GEEN DIRECTE SYSTEEMCOMPROMITTERING

De geïdentificeerde aandachtspunten vormen geen risico voor de beschikbaarheid, integriteit en vertrouwelijkheid van de geteste systemen.

- Er zijn geen aanwijzingen gevonden dat een aanvaller via deze aandachtspunten toegang kan realiseren of controle over het systeem kan verkrijgen.

ALGEHEEL BEELD

De uitgevoerde tests tonen aan dat zowel de SOAP- als REST-API-endpoints van “Pauzesignaal” en “SbEnSK versie 3” adequaat zijn beveiligd. De implementatie van authenticatie- en autorisatiemechanismen is conform de geldende standaarden, waarbij gevoelige gegevens afdoende worden beschermd. Tijdens het onderzoek zijn geen kwetsbaarheden aangetroffen die misbruik zonder geldige authenticatie mogelijk maken, noch zijn er aanwijzingen gevonden voor compromittering via directe systeemmanipulatie.

De resultaten van deze test vormen een momentopname. De beoordeling is uitgevoerd binnen een vooraf gedefinieerde scope en gedurende een specifiek tijdvak. Bevindingen hebben daarom uitsluitend betrekking op de onderzochte systemen en configuraties zoals deze op het moment van testen beschikbaar waren. Eventuele wijzigingen in infrastructuur, configuraties of processen na de testdatum vallen buiten de reikwijdte van deze resultaten.