ACA IT-Solutions, onderdeel van Crowe

COORDINATED VULNERABILITY DISCLOSURE

Documenttype:	**Adviesdocument**
Documentclassificatie:	**Publiek**
Documentnaam:	**Coordinated Vulnerability Disclosure ACA V1.0.pdf**
Naam opdrachtgever:	**Geert Rademakers (directie)**
Versie:	**1.0**
Datum opgesteld:	**maart-2021**
Datum definitief:	**31-12-2024**

ACA IT-Solutions, onderdeel van Crowe

Coordinated Vulnerability Disclosure-beleid
Elke dag werken specialisten bij ACA IT-Solutions aan het verbeteren van de systemen en processen, zodat de gegevens van onze klanten beschermd worden tegen misbruik, en de beschikbaarheid van de dienstverlening gewaarborgd is. Dat neemt niet weg dat zich ook in onze systemen kwetsbaarheden kunnen voordoen. Voor de waarneming hiervan maken we graag gebruik van uw hulp.

Wie kan melding maken van een kwetsbaarheid?
Iedereen die een mogelijke zwakke plek in de systemen van ACA IT-Solutions heeft ontdekt.

Wat is de scope?
Enkel de volgende domeinen (en alle onderliggende subdomeinen) vallen onder het Coordinated Vulnerability Disclosure-programma:

- aca-it.nl
- werktslim.com
- werkenbijaca.nl

Welke kwetsbaarheden kunt u melden?
U kunt problemen melden die gaan over de veiligheid van diensten die ACA IT Solutions aanbiedt via het internet. Voorbeeld van kwetsbaarheden die gemeld kunnen worden zijn:

- Remote Code execution
- Cross Site Scripting (XSS)-kwetsbaarheden
- Cross Site Request Forgery (CSRF)-kwetsbaarheden
- SQL-injectiekwetsbaarheden
- Kwetsbaarheden met betrekking tot encryptie
- Ongeautoriseerde toegang tot gegevens

Uitsluitingen

- Alle meldingen zonder een duidelijk rapport met het bewijs van mogelijke exploit
- Issues met betrekking tot SPF / DKIM / DMARC records
- Fingerprinting/versie banner disclosure op algemene/publieke services
- Publiek toegankelijke bestanden en mappen met niet gevoelige informatie (bijvoorbeeld robots.txt)
- Aanwezigheid van ‘autocomplete’- of ‘save password’-functionaliteit
- Cross Site Request Forgery (CSRF) kwetsbaarheden op statische pagina’s en logout-functionaliteit
- Bruteforce op ‘Wachtwoord vergeten’-pagina’s
- Redirection van HTTP naar HTTPS
- HTTP OPTIONS enabled
- Host Header Injection
- Ontbreken van HTTP Security Headers zoals: Strict-Transport-Security, X-Frame-Options, X-XSS-Protection, X-Content-Type-Options, Content-Security-Policy, X-Content
- Security-Policy, X-WebKit-CSP
- HTML does not specify charset
- HTML uses unrecognized charset

- Ontbreken van ‘Secure’ / ‘HTTP Only’ vlaggen op niet gevoelige cookies
- Clickjacking gerelateerde issues
- User enumeration op websites waar geen online betaaltransacties aanwezig zijn
- Mogelijk verouderde server- of applicatieversies (van externe partijen) zonder bewijs dat deze versies kwetsbaar zijn en bewijs van exploitatie.
- Rapporten van onveilige SSL-/ TLS-protocollen en andere misconfiguraties
- Generieke kwetsbaarheden gerelateerd aan software of protocollen die niet onder controle van ACA IT Solutions vallen
- Distributed Denial of Service (DDoS) aanvallen
- Spam- of Social Engineering-technieken
- Rapporten van reguliere scans, zoals poortscanners

Hoe moet u de melding doen?

Hebt u een kwetsbaarheid gevonden?

- Neem dan zo snel mogelijk contact met ons op via e-mail:
- Beschrijf het gevonden probleem zo uitgebreid mogelijk. Houd er rekening mee dat uw melding door specialisten wordt ontvangen; u kunt technisch jargon gebruiken waar nodig.
- U kunt ervoor kiezen om uw contactgegevens (naam en eventueel telefoonnummer) toe te voegen of u kunt de melding anoniem doen.

Wat doen we met uw melding?

Een team van beveiligingsexperts onderzoekt uw melding en geeft binnen twee werkdagen een eerste reactie. Maak het probleem in de tussentijd niet publiek, maar praat met onze experts en geef hen de tijd het probleem op te lossen. Wij laten u weten wat we van uw melding vinden, of we een oplossing gaan toepassen en wanneer we dat doen.

Beloning

Als dank ontvangt u een passende vergoeding voor kwetsbaarheden die we daadwerkelijk hebben kunnen verhelpen of die tot een verandering van de dienstverlening hebben geleid. Wij beslissen of de melding hiervoor in aanmerking komt en over de hoogte van de vergoeding. In het geval dat u in aanmerking komt voor een beloning, zullen wij uw persoonlijke gegevens nodig hebben om de betaling uit te kunnen voeren.

NB U kunt een kwetsbaarheid ook anoniem melden. Wij kunnen dan echter geen afspraken met u maken over de opvolging van uw melding, over een eventuele beloning en over het al of niet doen van aangifte (zie ‘Wat zijn de spelregels?’).

Wat zijn de spelregels?

Bij het onderzoeken van de kwetsbaarheid die u gevonden hebt, zou u mogelijk handelingen kunnen verrichten die strafbaar zijn. Als u te goeder trouw, zorgvuldig en volgens de aangegeven spelregels gehandeld hebt, is er voor ACA IT-Solutions geen aanleiding om aangifte te doen. Houdt u zich daarom aan de volgende regels wanneer u onderzoek doet:

- Zorg ervoor dat u met de gevonden kwetsbaarheid geen schade aanricht. In geen geval mag uw handelen leiden tot opzettelijke onderbreking van de dienstverlening of tot openbaarmaking klantgegevens.
- Maak geen gebruik van social engineering om toegang te verkrijgen tot een systeem.
- Gebruik geen geautomatiseerde scanners om kwetsbaarheden te vinden (zoals Burp Suite Scanner, Acunetix, etc).
- Plaats geen backdoor in een informatiesysteem om vervolgens daarmee de kwetsbaarheid aan te tonen, aangezien daarmee aanvullende schade kan worden aangericht en onnodige veiligheidsrisico's worden gelopen.
- Maak minimaal gebruik van een kwetsbaarheid, doe alleen datgene wat noodzakelijk is om de kwetsbaarheid vast te stellen.
- Wijzig of verwijder geen enkel gegeven van het systeem en wees zo terughoudend mogelijk met het kopiëren van gegevens (als één record genoeg is om het probleem aan te tonen, ga dan niet verder).
- Breng geen systeemveranderingen aan.
- Probeer niet herhaaldelijk toegang tot het systeem te verkrijgen en deel de verkregen toegang niet met anderen.
- Gebruik geen bruteforce om toegang tot systemen te verkrijgen. Daarbij is immers geen sprake van een kwetsbaarheid, maar alleen van het herhaaldelijk proberen van wachtwoorden.
- Een beloning zal alleen worden toegekend aan de eerste melder van de kwetsbaarheid.

Wat niet melden?

Het meldpunt cvd@aca-it.nl is niet bedoeld voor het:

- indienen van klachten over de dienstverlening van ACA IT-Solutions
- melden van fraude of vermoeden van fraude
- melden van nepmails of phishing e-mails
- melden van virussen
- indienen van klachten of vragen over de beschikbaarheid van de internetdiensten van ACA IT Solutions
- melden van problemen met geldautomaten

Uw privacy

Voor de opvolging van de melding kunt u ervoor kiezen om uw contactgegevens (naam, e-mail en eventueel telefoonnummer) aan ons te verstrekken. Wij gaan zorgvuldig om met uw persoonsgegevens. In ons Privacy Statement, dat u kunt vinden op aca-it.nl, leest u meer daarover.

Overige voorwaarden

Met betrekking tot internetveiligheid en privacy is de Nederlandse wetgeving van toepassing. Strafbare handelingen zullen mogelijk worden vervolgd. Wij kunnen alleen meldingen aannemen die in het Nederlands of Engels opgesteld zijn. Voor de uitkering van beloningen hebben wij uw persoonsgegevens nodig. Beloningen worden alleen uitgekeerd aan personen met een woonadres en bankrekening in Nederland. Mochten meerdere melders tegelijk dezelfde bevinding melden, dan is de vergoeding voor de eerste melder.