Coordinated Vulnerability Disclosure

Ben je deskundig en ontdek je een kwetsbaarheid in onze systemen? Help ons dan door deze kwetsbaarheid te melden. Zo kunnen we samen de veiligheid en betrouwbaarheid van onze systemen verbeteren.

Jeroen Bosch Ziekenhuis en veiligheid

Als Jeroen Bosch Ziekenhuis (JBZ) beschouwen we de veiligheid van onze websites en patiëntenportalen als topprioriteit. Ondanks alle tijd en moeite die we in de beveiliging van onze systemen steken, kunnen er nog steeds kwetsbaarheden in onze systemen aanwezig zijn.

Heb jij de juiste vaardigheden om zwakke plekken in onze systemen te kunnen ontdekken? Je kunt ons helpen door deze problemen te melden. Op die manier kunnen we de veiligheid en betrouwbaarheid van onze systemen verbeteren.

Een team van beveiligingsexperts zal jouw bevinding(en) onderzoeken. Binnen twee werkdagen ontvang je een e-mail met een eerste reactie. Het is echter mogelijk dat er een vertraging ontstaat bij het beantwoorden van je bevinding(en) als gevolg van werkdruk, feestdagen of vakantie.

Let op: Maak het probleem niet publiek voordat we het opgelost hebben. In plaats daarvan, praat met onze experts en geef hen de tijd het probleem op te lossen.

Waar is dit programma NIET voor bedoeld?

- Het indienen van klachten over de dienstverlening of producten van het JBZ
- Vragen of klachten over de beschikbaarheid van JBZ-websites of de patiëntenportalen
- Het melden van nepmails of phishing e-mails
- Het melden van virussen

De spelregels

Bij het onderzoek zou je mogelijk handelingen kunnen verrichten die strafbaar zijn. Als je te goeder trouw bent, zorgvuldig en volgens de aangegeven spelregels handelt, is er voor het JBZ geen aanleiding om aangifte te doen. Volg daarom de regels zoals opgenomen in deze coordinated vulnerability disclosure regeling en handel daarnaast niet op een onevenredige wijze:

- Zorg ervoor dat je tijdens het onderzoeken van de gevonden kwetsbaarheid geen schade aanricht.
- Maak geen gebruik van social engineering om toegang te krijgen tot een systeem.
- In geen geval mag jouw onderzoek leiden tot onderbreking van onze dienstverlening.
- In geen geval mag jouw onderzoek leiden tot openbaarmaking van ziekenhuis- of klantgegevens.
- Plaats geen backdoor in een systeem. Ook niet om de kwetsbaarheid aan te tonen. Door het plaatsen van een backdoor in een systeem, wordt dat systeem nog onveiliger.
- Wijzig of verwijder geen gegevens in het systeem. Is het voor het onderzoek nodig om gegevens uit het systeem te kopiëren? Kopieer dan nooit meer gegevens dan nodig. Als 1 record voldoende is voor jouw onderzoek, ga dan niet verder.
- Breng geen systeemveranderingen aan.
- Probeer niet vaker dan nodig een systeem binnen te dringen. Als het lukt om een systeem binnen te dringen, deel de toegang dan niet met anderen.

- Gebruik geen bruteforce-technieken (herhaaldelijk proberen van wachtwoorden) om toegang tot systemen te krijgen.
- Gebruik geen technieken die de beschikbaarheid van onze diensten kunnen beïnvloeden.

Beloning

We stimuleren je om gevonden kwetsbaarheden aan ons te rapporteren. Helaas krijg je hiervoor alleen de eer, we verstrekken geen beloning om bountyhunting te voorkomen.

Jouw privacy

JBZ en Z-Cert gebruiken je persoonsgegevens alleen om actie te ondernemen op jouw melding. We geven je persoonsgegevens niet zonder jouw toestemming aan anderen, tenzij wij op grond van de wet je gegevens moeten afstaan of als we een ander bedrijf inschakelen om jouw melding verder te onderzoeken. In dat geval zullen we er altijd voor zorgen dat ook zij op hun beurt op dezelfde manier als wij jouw gegevens geheim houden.

Hoe kun je een melding doen?

Je kunt een melding per e-mail doorgeven aan Stichting Z-Cert via CVD@z-cert.nl. Een voorwaarde voor het sturen van een e-mail naar bovengenoemd e-mailadres is dat de mail beveiligd wordt verstuurd. Je kan daarbij gebruik maken van de PGP-sleutel (https://www.z-cert.nl/pgp/). Schrijf je rapport op een duidelijke en beknopte manier. In het bijzonder:

- De stappen die je ondernam
- De volledige URL
- Wat de eventueel betrokken objecten zijn (bijvoorbeeld welke invoervelden of filters)
- Bewijs / hoe te reproduceren (video, schermafdruk indien mogelijk)
- Het risico of mogelijkheid tot uitvoering
- Het aanbieden van een oplossing wordt sterk aangemoedigd, maar niet verplicht

Onze specialisten lezen jouw melding en gaan gelijk aan de slag. Je krijgt direct een ontvangstbevestiging en binnen 5 dagen een reactie met verwachte datum van oplossing.

Als melder wordt je op de hoogte gehouden van je melding.

Wat kun je melden?

Voorbeeld van kwetsbaarheden die gemeld kunnen worden:

- 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

Uitgesloten is het melden van:

- Alle meldingen zonder een duidelijk rapport met het bewijs van mogelijke exploitatie
- Kwetsbaarheden gevonden op sites van organisaties die niet langer deel uitmaken van JBZ
- Ons beleid ten aanzien van de aanwezigheid of afwezigheid van SPF / DKIM / DMARC records
- Cross Site Request Forgery (CSRF) kwetsbaarheden op statische pagina's (alleen op pagina's na inloggen)
- Redirection van HTTP naar HTTPS
- HTML does not specify charset

- HTML uses unrecognized charset
- Cookie zonder HttpOnly vlag
- Geen gebruik van HTTP Strict Transport Security (HSTS)
- Clickjacking of de afwezigheid van X-Frame-Options op niet inlog pagina's
- Mogelijk verouderde server- of applicatie versies (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 JBZ vallen
- Distributed Denial of Service (DDoS) aanvallen
- Spam of Social Engineering technieken
- Rapporten van reguliere scans zoals poortscanners