Responsible Disclosure

ThreadStone Cyber Security vindt de veiligheid van de site heel belangrijk. Ondanks onze zorg voor de beveiliging van deze site kan het voorkomen dat er toch een zwakke plek is of is ontstaan.

Heb je een zwakke plek gevonden in de site www.threadstone.eu? Ben je er bijvoorbeeld per ongeluk tegenaan gelopen bij het normale gebruik van deze site? Of heb je expliciet je best gedaan om een zwakheid te vinden? Is de kwetsbaarheid opgenomen in de CVE database en heeft hij een CVSS score? Laat het ons weten zodat we zo snel mogelijk maatregelen kunnen nemen.

Dit is overigens geen uitnodiging om onze site uitgebreid te scannen en te testen om zwakke plekken te vinden. Dat doen we zelf wel. Ook testen op onze medewerkers of contractors (via social engineering), testen op applicaties van derden, testen op onze fysieke beveiliging, het uitvoeren van brute force aanvallen of het uitvoeren van denial of service aanvallen voeren we zelf uit. Hier hebben we dus geen ongevraagde hulp bij nodig.

We werken graag met je samen om de veiligheid van onze site nog beter te kunnen beschermen. We willen ons daarbij richten op de kwetsbaarheden die echt impact kunnen hebben. Daarom hebben we een aantal meldingen uitgesloten van deze Responsible Disclosure:

1. Meldingen die afkomstig zijn uit geautomatiseerde tools of scans;
2. Aanvallen die fysieke toegang tot het apparaat van een gebruiker vereisen;
3. Beleid voor wachtwoord- en accountherstel, zoals het resetten van een verlopen link of wachtwoordcomplexiteit;
4. Ontbrekende beveiligingsheaders die niet rechtstreeks leiden tot een kwetsbaarheid;
5. Clickjacking op statische websites;
6. Content spoofing/text injections;
7. Denial of service aanvallen welke alleen worden veroorzaakt door een grote hoeveelheid aanvragen;
8. Gebruik van een bekende kwetsbare bibliotheek (zonder dat er bewijs van misbruik is);
9. Problemen met betrekking tot software of protocollen die niet onder controle vallen van ThreadStone;
10. Meldingen van spam;
11. Kwetsbaarheden die gebruikers van verouderde of ongepatchte browsers en platforms beïnvloeden;
12. Social engineering van personeel of ingehuurde medewerkers (contractors);
13. Fysieke pogingen tegen datacenters of middelen van ThreadStone;
14. Eventuele meldingen over DKIM/DMARC/DNSSEC en SPF records.

Als je kwetsbaarheden hebt gevonden die binnen de reikwijdte van deze Responsible Disclosure valt vragen wij je:

1. Je bevindingen zo snel mogelijk te mailen naar info@threadstone.eu.
2. Voldoende informatie te geven om het probleem te reproduceren zodat we het zo snel mogelijk kunnen oplossen. Meestal is het IP-adres of de URL, een omschrijving van de kwetsbaarheid en een verwijzing naar de CVE database (bijvoorbeeld op www.cvedetails.com) voldoende, maar bij complexere kwetsbaarheden kan meer informatie nodig zijn.
3. De zwakheid niet te misbruiken door bijvoorbeeld veranderen of verwijderen van gegevens of het plaatsen van malware. Wij nemen uw melding altijd serieus en gaan elk vermoeden van een kwetsbaarheid uitzoeken.
4. Het probleem ook niet met anderen te delen totdat we het hebben opgelost.
5. Geen gegevens van onze systemen te kopiëren, anders dan absoluut noodzakelijk om het lek aan te tonen.
6. Contactgegevens (e-mail en telefoonnummer) achter te laten zodat we contact met je kunnen opnemen om samen te werken aan een veilig resultaat.

Wij beloven:

1. Binnen drie werkdagen te reageren op je melding met de beoordeling van de melding en een verwachte datum voor een oplossing.
2. Je melding vertrouwelijk te behandelen: we delen je persoonlijke gegevens niet zonder je toestemming. uitzondering hierop is politie en justitie, in geval van aangifte of als gegevens worden opgeëist.
3. Je op de hoogte te houden van de voortgang van het oplossen van het probleem.
4. Je in de berichtgeving omtrent het gemelde probleem, je naam te vermelden als ontdekker, als je dat wenst.
5. Dat een toevallig ontdekking in onze online-omgeving niet tot aangifte tegen je zal leiden. Zolang je je aan de spelregels houdt en je in de geest van Responsible Disclosure gedraagt, doen wij geen aangifte tegen je.
6. Als dank voor je hulp bieden wij een beloning aan voor elke melding van een ons nog onbekend beveiligingsprobleem. De grootte van de beloning bepalen we aan de hand van de ernst van het lek en de kwaliteit van de melding tot maximaal een bedrag van 500 euro.