Kwetsbaarheidsscan
voor de applicatie <naam applicatie>

Uitgevoerd door:

Datum:

Contents

Inleiding

Voor u ligt het rapport van de kwetsbaarheidsscan van de applicatie <naam applicatie>. In dit rapport wordt verslag gedaan van het onderzoek wat is uitgevoerd om vast te stellen of, en in welke mate de applicatie <naam applicatie> kwetsbaar is voor cybercriminele dreigingen.

Aanleiding

De aanleiding voor het uitvoeren van deze scan is <aanleiding>.

Beschrijving van de applicatie

<naam applicatie> is een onderdeel van de ICT van <naam bedrijf>. <naam applicatie> vervult de functie <naam functie>.

Risico

<naam applicatie> is wel/niet een bedrijfskritische applicatie.

Als deze applicatie getroffen zou worden door een cybercriminele aanval en om die reden niet meer operationeel betrouwbaar is, dan is de geschatte schade ongeveer <xxx euro> per <tijdseenheid>.

Methode

Het onderzoek bestaat uit drie fasen:

1. Het beschrijven van de applicatie:
    a. Functioneel
        i. (optioneel) het maken van een threat model
    b. Technisch
2. Online Database onderzoek naar bekende kwetsbaarheden
3. Het scannen van de applicatie met een of meerdere kwetsbaarheidsscanners (‘vulnerability scanner’)

Fase 1: Beschrijving van de applicatie

Fase 2: Online database onderzoek

Met de verkregen gegevens van fase 1 is een gericht onderzoek gedaan naar bekende kwetsbaarheden van de configuratie. Hiervoor is de CVE database[1] van MITRE geraadpleegd.

Fase 3: Scannen van de applicatie met kwetsbaarheidsscanners

De applicatie is gescand met gerenommeerde kwetsbaarheidsscanners. De scan is uitgevoerd onder hieronder uiteengezette omstandigheden. Er zijn meerdere tools gebruikt zodat de kans dat een kwetsbaarheid wordt gemist relatief klein is.

Testomstandigheden

De test is uitgevoerd terwijl de applicatie in een normale operationele situatie verkeerde. Voorafgaand aan de test is een volledige back-up gemaakt. Er was tijdens de test een technische en functionele beheerder aanwezig om bij calamiteiten de operatie te herstellen. De test is uitgevoerd buiten het interne netwerk van <naam bedrijf>. Het IP adres van de machine waarop de scan werd uitgevoerd is <IP-adres>.

De volgende scanners zijn gebruikt:

1. <naam scanner 1> , omdat..
2. <naam scanner 2> , vanwege …
3. <naam scanner 3> , …

[1] https://cve.mitre.org/cve/

Resultaten

Functionele beschrijving

Threat model

Technische beschrijving

Technische eigenschappen van <naam applicatie>

	Technologie	***Versie***	***Patch***
Framework / Stack			
…			
Data laag			
…			
API			
…			
Operating System			
…			

Online database onderzoek

Onderstaande tabel geeft het resultaat van deze inventarisatie weer. De gevonden CVE issues worden onder deze tabel toegelicht en beoordeeld op de mate van risico.

Technologie	***Versie***	***Patch***	***CVE***	***Issue #***

Bespreking van de veiligheidsrisico’s bij de aangetroffen CVEs

Issue #1

Issue #2

Kwetsbaarheidsscans

In deze paragraaf worden de resultaten van de applicatie scanners weergegeven.

<naam scanner 1>

<naam scanner 2>

Conclusie

De onderzoeken die zijn uitgevoerd schetsen het volgende beeld.

…

Om de beveiliging van de applicatie op een actueel niveau te brengen moeten de volgende maatregelen worden doorgevoerd.

Maatregelen