Vulnerability Assessment

Contasa

Prodicom B.V.
Robijnstraat 96
1812 RB Alkmaar

Inhoudsopgave

1 Inleiding

Voor je ligt het rapport met daarin de resultaten van de vulnerability assessment die door Prodicom is uitgevoerd.

Een vulnerability assessment brengt in kaart hoe het met de beveiliging van het IT-landschap is gesteld. Er wordt een scan uitgevoerd en uit de scan komen kwetsbaarheden naar voren. Tijdens de scan worden mogelijke doelwitten en systemen die voor hackers interessant kunnen zijn zichtbaar gemaakt. Dit kunnen bijvoorbeeld kwetsbaarheden zijn waar een hacker op kan inspelen om zich toegang te verschaffen tot het systeem of netwerk om vervolgens schade aan te richten, deze zaken komen met deze scan aan het licht mits deze aanwezig zijn in het landschap.

De kwetsbaarheden zijn gelabeld op de mate van ernst en in het rapport staan aanbevelingen met eventuele oplossingen. Deze rapportage zal ook mondeling toegelicht worden, het kan namelijk zo zijn dat een kwetsbaarheid op een systeem met een hoge mate van ernst minder problematisch voor het IT landschap is, dan een dan een kwetsbaarheid met een lage mate van ernst. Deze afweging zal in gezamenlijk overleg gemaakt moeten worden aangezien wij niet inzichtelijk hebben welke systemen bedrijfskritisch zijn.

2 Scan Scope

De scan is uitgevoerd met de aangeleverde login-gegevens. Op de aangeleverde ip-adressen. Hiermee is het mogelijk gemaakt om op de Windows machines in te kunnen loggen met als resultaat een nog gedetailleerder overzicht van welke kwetsbaarheden zich in het landschap bevinden.

Tijdens de intake kwam tevens naar voren dat er een goed overzicht is van de systemen en de daarbij behorende ip-adressen. Het is goed om te zien dat Contasa helder heeft welke systemen belangrijk zijn voor de primaire bedrijfsprocessen. Het resultaat hiervan is dat de aanbevelingen ook zijn geschreven op prioriteit van de belangrijkste systemen voor Contasa.

Hieronder vind je een overzicht van de verschillende netwerken die door Contasa zijn opgegeven.
Tevens vind je in de laatste kolom het aantal actieve apparaten wat wij gescand hebben in dit netwerksegment.

IP-Reeks	Functie van de Reeks	Gevonden apparaten
10.2.20.0/24	VOIP Segment	0
10.2.60.0/24	Production server Network	27
10.2.130.0/24	DMZ VLAN	2
10.2.10.0/24	Bekabeld LAN	12
10.2.105.0/24	Building Management VLAN	10

3 Samenvatting Resultaten

Normaal gesproken krijgen kwetsbaarheden een score door middel van het CVSS systeem.
Om dit overzichtelijker te maken kiezen wij er voor om ze op te delen in 4 categorieën in plaats van
een schaal van 1 tot 10. In de verdere rapportage staan ook de CVSS scores, hieronder staat een vertaal tabel van de CVSS score naar Severity score.

Severity level:	Info	Low	Medium	High	Critical
CVSS v2.0 score:	0	0,1–2,0	2,1–5,0	5,1–8,0	8,1–10
CVSS v3.x score:	0	0,1–2,0	2,1–5,0	5,1–8,0	8,1–10

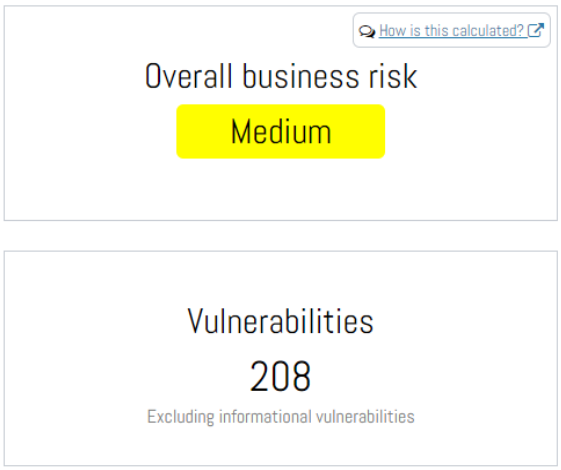
3.1 Overzicht Kwetsbaarheden binnen Contasa

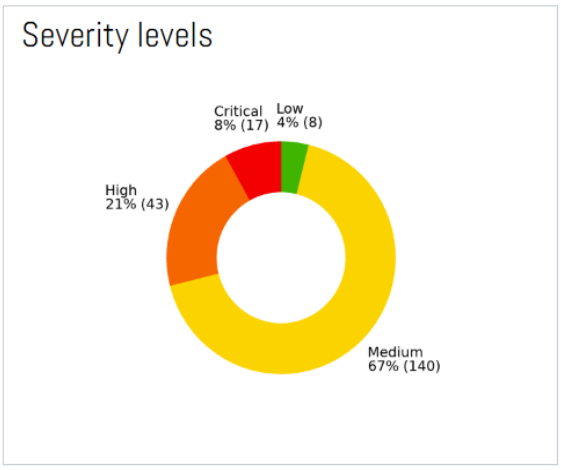
Dit overzicht is een weergave van hoeveel kwetsbaarheden er zijn gevonden in het landschap van Contasa . Dit zijn 208 kwetsbaarheden.

Het rechter overzicht geeft een weergave in welke severity categorie de kwetsbaarheden zich bevinden.

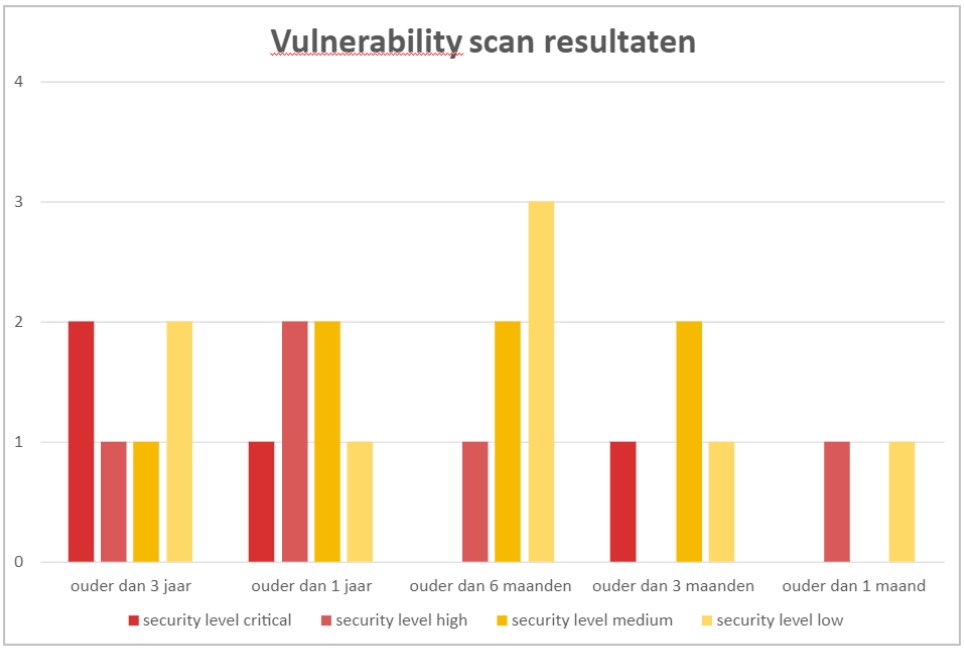
De overall business risk van Contasa is: Medium.

In de berekening van de business risk is ook de waarde van de asset meegenomen mits deze is opgegeven. Hoe deze waardes tot stand komen staat beschreven in hoofdstuk 8.1.





Onderstaande grafiek is een overzicht van de leeftijd van een kwetsbaarheid. Dit gaat dan om de datum dat de kwetsbaarheid publiekelijk is gepubliceerd. Dit is dus geen indicatie van hoe lang de kwetsbaarheid al aanwezig is in de omgeving bij Contasa is. Wat we kunnen concluderen uit deze grafiek is dat er op dit moment binnen Contasa geen actief vulnerability management wordt uitgevoerd.



4 Kwetsbaarheden

4.1 Critical kwetsbaarheden

CVSS Score	CVE ID (s)	Description	Solution	Count
10	CVE-2018-1160	Net-talk is prone to an unauthenticated code execution vulnerability.	Upgrade Net-talk to a version above version 3.1.12	1
9.3	CVE-2018-0598	Windows IExpress Untrusted Search Path Vulnerability	As a workaround save self-extracting archive files into a newly created directory, and confirm there are no unrelated files in the directory and make sure there are no suspicious files in the directory where self-extracting archive files are saved. Or remove Internet Explorer	14
9.3	CVE-2005-2936	Microsoft Windows Unquoted Path Vulnerability (SMB Login)	Software installing an 'Uninstall' registry entry or 'Service' on Microsoft Windows using an unquoted path containing at least one whitespace.	2

4.2 High Kwetsbaarheden

CVSS Score	CVE ID (s)	Description	Solution	Count
7.6	Multiple CVE's	Missing Windows Patches	Install the latest Windows Updates	15
6.9	CVE-2018-0598	Windows IExpress Untrusted Search Path Vulnerability	As a workaround save self-extracting archive files into a newly created directory, and confirm there are no unrelated files in the directory. Or remove Internet Explorer. It is EOL	14
9.3	CVE-2011-0638	a USB device driver software is prone to a code execution vulnerability.	No fix or work around. Microsoft doesn't warn the user before a HID is enabled	17
6.8	CVE-2020-15778	scp in OpenSSH through 8.3p1 allows command injectio	Update OpenSSH	7
5.8	CVE-2021-31439 , CVE-2022-0194 , CVE-2022-23121 , CVE-2022-23122 , CVE-2022-23123 , CVE-2022-23124 , CVE-2022-23125	Netatalk is prone to multiple vulnerabilities.	Netatalk versions before 3.1.13. are vulnerable. Update to versions higher then 3.1.13	1
5.8	No CVE ID	The host has enabled SMBv1 for SMB	Disable SMBv1 and use SMBv2 even better is SMBv3	1
5.8	CVE-2018-20685 , CVE-2019-6109 , CVE-2019-6110 , CVE-2019-6111	OpenBSD OpenSSH is prone to multiple vulnerabilities.	Update to a higher version of OpenBSD OpenSSH versions 7.9	1

4.3 Medium Kwetsbaarheden

CVSS Score	CVE ID (s)	Description	Solution	Count
5.0	Multiple CVE's	Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSH, D(HE)ater)	DHE key exchange should be disabled	35
5.0	CVE-2016-2183 , CVE-2016-6329 , CVE-2020-12872	SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.	6
5.0	No CVE Number	DCE/RPC and MSRPC Services Enumeration Reporting	DCE/RPCshould be updated to the latest version. -> Allow only whitelisted local IP addresses to access port 135. -> Filter incoming traffic to port 135.	16
5.0	CVE-2021-33500	PuTTY < 0.75 DoS Vulnerability	Update Putty to the latest version	1
4.6	CVE-2021-28041	OpenSSH 8.2 < 8.5 Memory Corruption Vulnerability	Update to version 8.5 or later.	6

5 Aanbevelingen

Na dat wij de scanresultaten hebben geanalyseerd komen wij tot de conclusie dat het IT-Landschap van Contasa in goede staat verkeerd. Wel zien wij een probleem bij het beheer van de middelware applicaties zoals bijvoorbeeld Putty en Microsoft Office applicaties. Deze moeten vaker gecontroleerd worden of deze up-to-date zijn. Verder lijkt het er op dat een op een aantal Windows servers de Windows updates al enige tijd niet zijn geïnstalleerd.

Wij hebben de firewall helaas niet geauthentiseerd kunnen scannen dit omdat wij geen login gegevens hebben ontvangen voor de firewall, desondanks komen er toch kwetsbaarheden naar voren. Die een Critical Severity hebben. Hieruit kunnen wij opmaken dat er al enige tijd geen patches zijn geïnstalleerd op de Netwerkapparatuur.

Verder is ons advies om SMBv1 binnen de organisatie uit te zetten, dit is een verouderd protocol wat vaak door hackers wordt gebruikt, uit onze scan zijn geen Windows 7 en Windows server 2008 machines naar voren gekomen. Het is dus mogelijk om over te stappen op SMBv3. Mocht dit niet kunnen dan is SMBv3 voor nu ook afdoende.

Zoals in de rapportage terug te vinden is zijn er nog een aantal Windows 7 werkstations actief in het netwerk van Contasa. Ons advies is om deze zo snel mogelijk te vervangen of als deze niet te vervangen zijn door bijvoorbeeld legacy software deze machines zo veel mogelijk te isoleren van het netwerk. Prodicom kan hierbij eventueel ondersteunen.

Tijdens de finding-meeting zullen wij de resultaten doorspreken en tevens een voorstel doen welke zaken als eerste dienen opgepakt te worden.

6 Open poorten

Tijdens de scan die is uitgevoerd zijn tijdens de scan de volgende poorten gedetecteerd die in verband staan met een gevonden kwetsbaarheid in de omgeving:

Port	Type	Assets	Vulnerabilities	Severity Level
49152	TCP	2	6	Critical
445	TCP	4	23	Critical
49161	TCP	1	1	Medium
135	TCP	4	7	Medium
22	TCP	2	12	Medium
49153	TCP	1	1	Medium
49154	TCP	1	1	Medium
443	TCP	2	9	Medium
8443	TCP	1	5	Medium
3389	TCP	1	9	Medium
49155	TCP	1	1	Medium
8834	TCP	1	17	Medium
49156	TCP	1	1	Medium

7 Uitgebreide scan rapportage

Bij deze scan leveren wij een drietal uitgebreide rapportages. De eerste rapportage bestaat uit een
overzicht van de kwetsbaarheden met daarbij de systemen die deze kwetsbaarheden hebben. De tweede rapportage bestaat uit een overzicht van de gescande systemen met de daarbij gevonden kwetsbaarheden. De laatste rapportage is een Excel (.csv) File welke makkelijk doorzoekbaar is en tevens kunnen hier ook filters op toegepast worden

8 Bijlages

8.1 Vertaaltabel Business risk

Business risk

	Critical	**High**	**Medium**	**Low**	**Severity**
High	Critical	High	Medium	Medium	
Medium	High	Medium	Medium	Low	
Neutral	Medium	Medium	Low	Low	
Low	Medium	Low	Low	Low	

Business impact