VULNERABILLITY ASSESMENT

RAPPORT & TOELICTHING

PRISMA-RT Nederland

Versie	1.0
Publicatiedatum	08-05-2015
Laatste wijziging	31 mei 2016
Auteur(s)	Jeffrey de Boer

Table of Contents

Vulnerabillity met uitleg

Title	Severity	CVSS Score
TLS/SSL Server Supports DES and IDEA Cipher Suites	Medium	5.8

Vulnerabillity: Gekozen TLS versie ondersteund DES en IDEA Cipher Suites.

Uitleg: De scanner controleert welke TLS/SSL protocol er word gekozen en/of geforceerd door de web server en controleert dan welke Encryptie methoden worden gebruikt daarin en of deze nog veilig zijn. In dit geval heeft is de scanner opgevallen dat op de Web Server TLS versie 1.1 word gekozen waarin ondersteuning zit voor oudere encryptie technieken als DES en IDEA.

Toelichting TPSC: Wij kiezen ervoor om TLS versie 1.1 te ondersteunen zodat wij klanten met oudere browser versies, met name Internet Explorer, niet uitsluiten. In sommige oudere browsers zit er namelijk nog geen ondersteuning voor TLS 1.2. Die word overigens wel ondersteun door onze Web Server en zal, indien beschikbaar bij de cliënt, ook worden geforceerd.

Wij hebben daarbij op de webserver aangegeven dat dat de voorkeur uitgaat naar AES ciphers.

Title	Severity	CVSS Score
TCP Sequence Number Approximation Vulnerability	Medium	5.0

Vulnerabillity: Er kan, bij grote data transfers, een schatting gemaakt worden naar de Sequence nummers in een TCP segment.

Uitleg: Bij een grotere window size, bij het sturen van veel data, zou het mogelijk zijn om het Sequence nummer van een TCP segment te raden. Dit kan door constant TCP RST packets te sturen naar de server. Dit komt voornamelijk voor in protocollen waarbij connectie lang openstaat zoals BGP.

Toelichting TPSC: Wij maken geen gebruik van het BGP Protocol. Waarbij hebben wij meerdere time-outs ingesteld waarbij het niet mogelijk is om de sequence te raden. Tevens hebben wij bij de host een Intrustion Prevention System draaien die ervoor moet zorgen dat men niet herhaaldelijk dit soort pakketten kan insturen.

Title	Severity	CVSS Score
TLS Server Supports TLS version 1.0	Medium	4.3

Vulnerabillity: Web Server ondersteund TLS versie 1.0

Uitleg: TLS 1.0 is een verouderde protocol voor https (ssl) verkeer. Daarin worden verouderde encryptie technieken als DES gevoerd.

Toelichting TPSC: TLS 1.0. is uitgezet na deze constatering. Vanaf heden ondersteuning wij alleen TLS 1.1 en TLS 1.2.

Title	Severity	CVSS Score
TLS/SSL Server Supports Cipher Block Chaining (CBC) Ciphers	Low	2.6

Vulnerabillity: Web Server ondersteund Cipher Block Chaining.

Uitleg: CBC is een encryptie techniek die gebruikt word in alle TLS en SSL versies behalve TLS versie 1.3. Hierbij word de BIT Stream (zeg maar, pakket stroom) opgedeeld in stukken en geencrypt met een Initialization Vector (IV). Als er daarbij van een voorspelbare IV word gekozen is het mogelijk om, met een bepaalde aanval, bijv. cookies op te halen. Dit noemt met een "BEAST" attack.

Toelichting TPSC: In oude SSL versies en in TLS 1.0 werden er Zero Initilization Vectors en zwakke IV's gebruikt. Hierdoor waren deze versies van SSL/TLS kwetsbaar. Vanaf TLS versie 1.1 is dit opgelost. Dit is de versie van TLS die wij hoofdzakelijk voeren.

Title	Severity	CVSS Score
TLS/SSL Server Supports The Use of Static Key Ciphers	Low	2.6

Vulnerabillity: De Web Server ondersteund Static Key Ciphers. Dit is een mogelijkheid in TLS 1.0

Uitleg: Dit word als een vulnerabillity gezien omdat met Static Keys er geen ondersteuning is voor "Foward Secrecy". Vanaf TLS 1.1 is het gebruik van Static Ciphers weg gehaald.

Toelichting TPSC: Helaas ondersteunen oudere browsers geen Forward Secrecy, die wij wel standaard aanbieden. TLS 1.0 is uitgezet, daarbij zou deze vulnerabillity zijn verdwenen.

Title	Severity	CVSS Score
TLS/SSL Server Is Using Commonly Used Prime Numbers	Low	2.6

Vulnerabillity: Bij het gebruik van de Diffie-Hellman key exchange (encryptie techniek) word er gebruik gemaakt van priem-getallen.

Uitleg: De parameter van de Diffie-Hellman key exchange word vaak gebaseerd op een priem getal. Het zou dan theoretisch mogelijk zijn om een zogeheten rainbow table te maken waarin men de shared secret voor de handshake kan achterhalen.

Toelichting TPSC: Dit is tot op heden alleen in theorie mogelijk. Tot op heden heeft niemand nog de computing power en tijd gehad om daadwerkelijk een werkbare rainbow table te maken waarin een handshake van de Diffie-Hellman suite kan worden achterhaald.

Title	Severity	CVSS Score
TLS Server Supports TLS version 1.1	Low	2.6

Vulnerabillity: De webserver ondersteund TLS versie 1.1

Uitleg: De webserver ondersteund TLS versie 1.1.

Toelichting TPSC: Voor de PCI DSS Accreditatie is het gebruikelijk om TLS 1.2 te forceren. ER is echter geen aantoonbaar bewijs dat TLS 1.1 kwetsbaarheden bevat. Het is echter, specifiek voor die accreditatie, gebruikelijk om alleen de nieuwste TLS versie forceren.

Daarbij ondersteunen heel veel oudere browser versies TLS 1.2, of althans de encryptie suites die daarin gebruikt worden, niet.

IP Address	Port	Proof
134.0.76.70	443/tcp	Successfully connected to 134.0.76.70:443 over TLSv1.1

Vulnerabillity: Men kon, in tegenstelling tot TLS 1.0, een succesvolle connectie maken via TLS 1.1 met de diensten die op de web server draaien.

Uitleg: Er kon een connectie worden gemaakt met de TPSC applicatie via TLS 1.1. Dit word nu als vulnerabillity geflagged omdat het in PCI DSS gebruikelijker is om TLS 1.2 te hanteren.

Toelichting TPSC: Zie de bovenstaande Vulnerabillity voor meer uitleg omtrent TLS 1.1. Het klopt dat deze connectie toegestaan word, die als veilig word gezien.