
TC037

BEHEER VAN CIPHER SUITES

Heeft het issue impact op..?	
Grootverbruik	X
Kleinverbruik	X
Elektriciteit	X
Gas	X
RNB	X
LNB	X
LV	X
MV	X
PV	X
EDSN	X
Codes	
Berichten	
Ketenprocessen	
Privacy	
Is het issue release afhankelijk/onafhankelijk en welke invoeringsdatum heeft het issue.	
Release-afhankelijk	
Release-onafhankelijk	X

Nummer TC037
Datum 05-07-2017
Versie 1.0
Status Ter vaststelling

Opsteller(s) Gerrit Fokkema
Ed van der Pijl

Inhoudsopgave

Colofon	3
Versiebeheer	3
Distributie	3
Probleemdefinitie	4
Overwegingen	5
Gekozen oplossing	5
Impact	5
Invoeringsstrategie	6
Te vervallen issues	6

COLOFON

VERSIEBEHEER

Versie	Status	Wijziging	Auteur	Datum
0.1	Concept	Eerste opzet, na meerdere besprekingen in de TC	Gerrit Fokkema , Ed v.d. Pijl	05-05-2017
0.2	Concept	Kleine aanscherpingen na bespreking in de TC van 12-05-2017	Gerrit Fokkema	18-05-2017
0.3 en 0.9	Ter vaststelling	Redactionele puntjes n.a.v. review door de Security Commissie	Gerrit Fokkema	01-06-2017
1.0	Vastgesteld	Na vaststelling in de ALV van 05-07-2017	Gerrit Fokkema	05-07-2017

DISTRIBUTIE

Gremium	Verstuurd (versie/datum)									
	0.1	0.2	0.3	0.4	0.5	0.6	0.70	0.8	0.9	1.0
	dd-mm-jjjj	dd-mm-jjjj	dd-mm-jjjj	dd-mm-jjjj	dd-mm-jjjj	dd-mm-jjjj	dd-mm-jjjj	dd-mm-jjjj	dd-mm-jjjj	dd-mm-jjjj
TC	05-05-2017	18-05-2017	01-05-2017							
SC		18-05-2017								
SPC			01-05-2017							
ALV NEDU			23-05-2017						01-06-2017	05-07-2017
Allen										

PROBLEEMDEFINITIE

Onderdeel	Omschrijving
De ontwikkeling betreft:	In de rat-race van de beveiliging is van belang bij te blijven bij de ontwikkelingen. Dit geldt zeker ook bij de beveiliging van de verbindingen die worden gelegd voor de communicatie in de ketenprocessen in de sector. De verbindingen worden sinds enige tijd beveiligd met TLS1.2. Hierbinnen wordt gebruik gemaakt van SHA256 certificaten en versleutelingen, waarvoor diverse algoritmes kunnen worden gebruikt, die worden gekenmerkt als ciphersuites. Met regelmaat worden bepaalde ciphersuites gekraakt en zijn niet meer veilig te gebruiken. Zo nu en dan worden nieuwe, veiliger suites gelanceerd. Het is van belang deze ontwikkelingen te volgen.
En raakt:	Alle verbindingen tussen marktpartijen die gebruikt worden voor de ketenprocessen.
Als gevolg waarvan:	De beveiligingsgraad continu onder druk staat
Een goede oplossing moet:	Een hanteerbaar proces opleveren dat de lijn beveiliging op voldoende niveau houdt.
Of deze doelen worden behaald, kan worden gevalideerd door:	Een proces wordt afgesproken dat functioneert.
Opdrachtgever te realiseren oplossing	NEDU
Probleemeigenaar	TC

OVERWEGINGEN

De sector maakt gebruik van verbindingen onder TLS 1.2 (zie TC024), die onder andere wordt beveiligd met SHA256 certificaten en het gebruik van een set aan toegestane ciphersuites voor de beveiligingsalgoritmes.

Er bestaat een aantal internationale en nationale instanties die de ontwikkelingen op het terrein van security volgen en daar adviezen en richtlijnen voor publiceren (zoals de ENISA vanuit de EU, ISAC en de Energie-ISAC in Nederland en de Amerikaanse Common CVE, Vulnerabilities and Exposures, databank).

De Security Commissie volgt en is aangehaakt bij een aantal van deze instanties en zal periodiek evalueren welke ciphersuites niet meer veilig genoeg zijn om te gebruiken in de beveiliging van de verbindingen in de sectorale informatieuitwisseling.

De technische commissie zal op basis hiervan aangeven hoe om te gaan met de ciphersuites en zo nodig andere beveiligingen in de verbindingen.

GEKOZEN OPLOSSING

De Security Commissie evalueert periodiek, tenminste eenmaal per jaar de in gebruik zijnde ciphersuites en geeft aan welke niet meer gebruikt dienen te worden.

De Technische Commissie beheert de lijst van de in de ketencommunicatie te gebruiken ciphersuites en zal op basis van de bevindingen van de Security Commissie acties inplannen om de onveilige ciphersuites uit productie te laten nemen. Daartoe zal een TC issue worden opgesteld met formele besluitvorming en inplanning. Mogelijk dat er later een meer regulier, operationeel proces van kan worden gemaakt.

Tevens zal communicatie richting de gekende functioneel beheerders van de marktpartijen worden gedaan.

Let wel dat deze procedure *niet* wordt gebruikt bij calamiteiten, waarbij het kan zijn dat op zeer korte termijn ciphersuites dienen te worden uitgefaseerd.

IMPACT

Geen impact op code of DPM.

INVOERINGSSTRATEGIE

	Release onafhankelijk	Release afhankelijk
Na vaststelling ALV NEDU	X	
Sectorrelease		
Specifieke datum		

De procedure kan meteen na vaststelling door de ALV van kracht worden.

TE VERVALLEN ISSUES

Nvt