TC038

Jaarlijkse update 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 TC038
Datum 23-05-2018
Versie 3.0
Status Vastgesteld

Opsteller(s) Wim de Olde (GTS)

Inhoudsopgave

Colofon

Versiebeheer

Versie	Status	Wijziging	Auteur	Datum
0.1	Concept	Eerste opzet op basis van input van de SC	Wim de Olde	22-11-2017
0.2	Ter vaststelling	Aanscherpingen nav bespreking in de TC vergadering van 15 december 2017	Wim de Olde	15-12-2017
1.0	Vastgesteld ALV 17-01-2018-	Geen	Gerrit Fokkema	5-02-2018
1.1	Ter vaststelling	Release afhankelijk + schrijfwijzen ciphersuites toegevoegd, advies nog aangepast.	Wim de Olde	16-03-2018
2.0	Vastgesteld door de ALV		Gerrit Fokkema	11-04-2018
2.1	Concept	Aanscherping met gedoogperiode voor de DHE suites onder RSA en GCM	Gerrit Fokkema, Wim de Olde	07-05-2018
2.2	Ter vaststelling	Tekstuele aanscherpingen na review door de TC leden	Gerrit Fokkema	15-05-2018
3.0	Vastgesteld door de ALV		Gerrit Fokkema	23-05-2018

Distributie

Gremium	Verstuurd (versie/datum)									
	0.1	0.2	1.0	1.1	2.1	2.2	3.0			
TC	22-11-2017	15-12-2017		16-03-2018	07-05-2018					
SC		15-12-2017								
SPC		22-12-2017								
ALV NEDU		09-01-2018		04-04-2018		15-05-2018				
Allen			05-02-2018				23-05-2018			

1 Probleemdefinitie

Onderdeel	Omschrijving
Het probleem betreft:	Het gebruik van onveilige cipher suites voor de beveiliging (via TLS) van de verbindingen in ketenprocessen
En raakt:	Alle met TLS beveiligde verbindingen tussen marktpartijen die gebruikt worden voor ketenprocessen
Als gevolg waarvan:	De beveiligingsgraad onder druk staat
Een goede oplossing moet:	Een lijst cipher suites opleveren die voldoende veilig zijn
Of deze doelen worden behaald, kan worden gevalideerd door:	Uitvraag te doen bij de marktpartijen
Opdrachtgever te realiseren oplossing	NEDU
Probleemeigenaar	Technische Commissie

2 Overwegingen

In TC037 Beheer van cipher suites is een proces afgesproken om in gebruik zijnde cipher suites te evalueren en onveilige cipher suites uit productie te nemen. In dit proces heeft de Security Commissie de taak om de cipher suites te evalueren en de Technische Commissie om onveilige cipher suites uit productie te laten nemen.

De Security Commissie heeft de cipher suites zoals toegepast in het TLS1.2 protocol (TC024) geëvalueerd en deze evaluatie gedeeld met de Technische Commissie. De Technische Commissie volgt het advies van de Security Commissie om een deel van de cipher suites als ‘goed’ te kwalificeren en een deel als ‘voldoende’.

3 Gekozen oplossing

3.1 TLS 1.2 cipher suite advies 2017-2018

Cipher Group	Prio	TLS ID1	TLS ID2	CipherName	Name (OpenSSL)	Cipher Suite Name (RFC)
Goed	1	0xc02c	0xC0 0x2C	TLS(1.2)-ECDHE-ECDSA-AES256-GCM-SHA384	ECDHE-ECDSA-AES256-GCM-SHA384	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
	2	0xc02b	0xC0 0x2B	TLS(1.2)-ECDHE-ECDSA-AES128-GCM-SHA256	ECDHE-ECDSA-AES128-GCM-SHA256	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
	3	0xc030	0xC0 0x30	TLS(1.2)-ECDHE-RSA-AES256-GCM-SHA384	ECDHE-RSA-AES256-GCM-SHA384	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
	4	0xc02f	0xC0 0x2F	TLS(1.2)-ECDHE-RSA-AES128-GCM-SHA256	ECDHE-RSA-AES128-GCM-SHA256	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
	5	0x9d	0x00 0x9D	TLS(1.2)-AES256-GCM-SHA384	AES256-GCM-SHA384	TLS_RSA_WITH_AES_256_GCM_SHA384
	6	0x9c	0x00 0x9C	TLS(1.2)-AES128-GCM-SHA256	AES128-GCM-SHA256	TLS_RSA_WITH_AES_128_GCM_SHA256
	7	0x9f	0x00 0x9F	TLS(1.2)-DHE-RSA-AES256-GCM-SHA384	DHE-RSA-AES256-GCM-SHA384	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
	8	0x9e	0x00 0x9E	TLS(1.2)-DHE-RSA-AES128-GCM-SHA256	DHE-RSA-AES128-GCM-SHA256	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
Voldoende	9	0xc024	0xC0 0x24	TLS(1.2)-ECDHE-ECDSA-AES256-SHA384	ECDHE-ECDSA-AES256-SHA384	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
	10	0xc023	0xC0 0x23	TLS(1.2)-ECDHE-ECDSA-AES128-SHA256	ECDHE-ECDSA-AES128-SHA256	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
	11	0xc028	0xC0 0x28	TLS(1.2)-ECDHE-RSA-AES-256-SHA384	ECDHE-RSA-AES256-SHA384	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
	12	0xc027	0xC0 0x27	TLS(1.2)-ECDHE-RSA-AES-128-SHA256	ECDHE-RSA-AES128-SHA256	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
	13	0x3d	0x00 0x3D	TLS(1.2)-AES-256-SHA256	AES256-SHA256	TLS_RSA_WITH_AES_256_CBC_SHA256
	14	0x3c	0x00 0x3C	TLS(1.2)-AES-128-SHA256	AES128-SHA256	TLS_RSA_WITH_AES_128_CBC_SHA256
	15	0x6b	0x00 0x6B	TLS(1.2)-DHE-RSA-AES-256-SHA256	DHE-RSA-AES256-SHA256	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
	16	0x67	0x00 0x67	TLS(1.2)-DHE-RSA-AES-128-SHA256	DHE-RSA-AES128-SHA256	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

In de drie rechtse kolommen zijn de verschillende schrijfwijzen gegeven.
Identificatie vindt plaats via het TLS ID, hier zijn twee methodes voor, aangegeven als TLS ID1 resp. TLS ID2. In een aantal gevallen worden voor TLS ID1 zes posities gebruikt door op te vullen met voorloopnul(len); bijv.: ‘0x9d’ = ‘0x009d’.

Referenties:

https://testssl.sh/openssl-rfc.mapping.html;
https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml;

https://www.openssl.org/docs/manmaster/man1/ciphers.html.

Het verdient de aanbeveling om de cipher suites ook in bovenstaande volgorde aan te bieden.

Er wordt aangetekend dat

- de CBC cipher suites vervangen dienen te worden door de GCM suites;
- Diffie Helman keys (DHE) dienen te worden uitgefaseerd.

Dit is technisch nog niet altijd mogelijk vanwege gebruikte software of zelfs hardware, vandaar dat de TC in 2018 de huidige set wil behouden.

3.2 TLS 1.2 cipher suite advies 2019

De TC vraagt de ALV NEDU te besluiten tot het overgaan naar alleen ECDHE en GCM cipher suites per 1-1-2019. Sommige partijen zullen hun software mogelijk moeten upgraden om de CBC cipher suites uit te faseren. In volgorde van security en algemeen gebruik geldt dan (zie tabel): **vetgedrukt**: de meest veilige set; normaal gedrukt: veilig (en de gedoog suites voor 2019); *schuingedrukt*: nog matig veilig (CBC) en de overige niet meer gebruiken (DHE).
Om overgangsproblemen te voorkomen wordt voorgesteld om de twee DHE-RSA suites i.c.m. GCM, als aangegeven in de tabel, tijdelijk in 2019 te gedogen.

Cipher Group	Prio	TLS ID1	TLS ID2	CipherName	Name (OpenSSL)	Cipher Suite Name (RFC)
Goed	**1**	**0xc02c**	**0xC0 0x2C**	**TLS(1.2)-ECDHE-ECDSA-AES256-GCM-SHA384**	**ECDHE-ECDSA-AES256-GCM-SHA384**	**TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384**
	2	**0xc02b**	**0xC0 0x2B**	**TLS(1.2)-ECDHE-ECDSA-AES128-GCM-SHA256**	**ECDHE-ECDSA-AES128-GCM-SHA256**	**TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256**
	3	**0xc030**	**0xC0 0x30**	**TLS(1.2)-ECDHE-RSA-AES256-GCM-SHA384**	**ECDHE-RSA-AES256-GCM-SHA384**	**TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384**
	4	**0xc02f**	**0xC0 0x2F**	**TLS(1.2)-ECDHE-RSA-AES128-GCM-SHA256**	**ECDHE-RSA-AES128-GCM-SHA256**	**TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256**
	5	0x9d	0x00 0x9D	TLS(1.2)-AES256-GCM-SHA384	AES256-GCM-SHA384	TLS_RSA_WITH_AES_256_GCM_SHA384
	6	0x9c	0x00 0x9C	TLS(1.2)-AES128-GCM-SHA256	AES128-GCM-SHA256	TLS_RSA_WITH_AES_128_GCM_SHA256
Tijdelijk in 2019	7	0x9f	0x00 0x9F	TLS(1.2)-DHE-RSA-AES256-GCM-SHA384	DHE-RSA-AES256-GCM-SHA384	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
	8	0x9e	0x00 0x9E	TLS(1.2)-DHE-RSA-AES128-GCM-SHA256	DHE-RSA-AES128-GCM-SHA256	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
Matig	*9*	*0xc024*	*0xC0 0x24*	*TLS(1.2)-ECDHE-ECDSA-AES256-SHA384*	*ECDHE-ECDSA-AES256-SHA384*	*TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384*
	10	*0xc023*	*0xC0 0x23*	*TLS(1.2)-ECDHE-ECDSA-AES128-SHA256*	*ECDHE-ECDSA-AES128-SHA256*	*TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256*
	11	*0xc028*	*0xC0 0x28*	*TLS(1.2)-ECDHE-RSA-AES-256-SHA384*	*ECDHE-RSA-AES256-SHA384*	*TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384*
	12	*0xc027*	*0xC0 0x27*	*TLS(1.2)-ECDHE-RSA-AES-128-SHA256*	*ECDHE-RSA-AES128-SHA256*	*TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256*
	13	*0x3d*	*0x00 0x3D*	*TLS(1.2)-AES-256-SHA256*	*AES256-SHA256*	*TLS_RSA_WITH_AES_256_CBC_SHA256*
	14	*0x3c*	*0x00 0x3C*	*TLS(1.2)-AES-128-SHA256*	*AES128-SHA256*	*TLS_RSA_WITH_AES_128_CBC_SHA256*

Actie: Het voorstel is om in september 2018 een uitvraag te doen of partijen gereed zijn om de CBC en DHE cipher suites uit te sluiten.

4 Impact

Partijen bereiden het uitfaseren van CBC en DHE cipher suites per 1-1-2019 in hun landschap voor. Voor twee DHE suites (zie tabel) wordt gedurende 2019 een uitzondering gemaakt, deze zijn per einde 2019 niet meer toegestaan.

5 Invoeringsstrategie

	Release onafhankelijk	**Release afhankelijk**
Na vaststelling ALV NEDU		
Sectorrelease		
Specifieke datum	01-01-2019	

6 Te vervallen issues

NVT