Voorstel om verstrekking sha-1-certificaten te verlengen is ingetrokken

Door Olaf van Miltenburg, dinsdag 13 oktober 2015 21:13, 38 reacties • Feedback

Het voorstel bij het CA /Browser Forum om de uitgifte van sha-1-certificaten met nog een jaar te verlengen is ingetrokken. De intrekking volgt op een oproep van cryptologen om de standaard versneld uit te faseren omdat deze sneller te kraken blijkt dan gedacht.

Het voorstel om te stemmen voor een verlenging was door Symantec ingediend bij het Certification Authority Browser Forum van certificaatautoriteiten en browserbouwers en het werd ondersteund door Microsoft en Trend Micro. De indieners trekken Ballot 152 echter terug.

De intrekking volgt op een oproep van een team van cryptologen, waaronder de Nederlander Marc Stevens, om sneller te stoppen met de sha-1-standaard. Het team had aangetoond dat een collision-aanval op de hashingstandaard relatief goedkoop en in enkele maanden uitgevoerd kan worden - veel sneller dan gedacht - door gebruik te maken van een grote hoeveelheid gpu's.

De uitkomst van het onderzoek heeft mogelijk ook gevolgen voor de tls 1.3-standaard. In het voorstel voor die komende standaard voor versleutelde internetverbindingen is nu opgenomen dat sha-1 met signatures heeft afgedaan. Hierover ontstond een discussie bij de Transport Layer Security-werkgroep van de IETF. Sha-1 is een hashing-algoritme uit 1995 dat nog altijd veel gebruikt wordt voor de certificaten voor software en ssl/tls-authenticatie. Al jaren geleden zijn kwetsbaarheden in het algoritme blootgelegd.

Delen

AIVD: terroristen hebben te weinig capaciteiten om te hacken
App Store van Apple kampt met storing - update

Reacties (38) Gerelateerd

Reacties (38)

Moderatie-faq • Wijzig weergave

-1	0	+1	+2	+3	Ongemodereerd
38	38	36	6	0	0

CAPSLOCK2000 +2
14 oktober 2015 00:21

Gelukkig maar, hoe langer we SHA-1 in leven houden hoe groter we het probleem maken. We weten dat het nog jaren zal duren voor het echt niet meer gebruikt wordt. Voorganger MD5 is ook nog steeds in gebruik en dat is echt niet meer te vertrouwen.

Ik zou ook graag meer support voor andere hash-algoritmes. Meestal is SHA-2 nu de enige reëele mogelijkheid. Als er een probleem gevonden wordt met SHA-2 hebben we in veel gevallen geen alternatief.

netdata +1
13 oktober 2015 21:20

Vind het zowiso al frapant dat een deel van de grote spelers nog steeds SHA1 certificaten gebruikt.
Ik denk hierbij bijvb aan:

- https://login.live.com
- https://www.cloudflare.com/a/login

Bjornmeijer935
@netdata • 13 oktober 2015 22:20

+2

Het is overigens niet zo dat ze sha1 certificaten gebruiken, het zijn sha2(256) certificaten echter worden sha1 cipher suites nog steeds geaccepteerd waardoor het dus werkt voor sha1 clients.

Plopeye
@Bjornmeijer935 • 14 oktober 2015 04:49

+1

SHA De H in deze reeks letters staat voor Hashing en SHA1 is dus geen cipher!

Compizfox
@Plopeye • 14 oktober 2015 10:53

+2

Dat zegt hij toch ook niet?

Hij zegt dat er cipher suites met SHA1 ondersteund worden. Een cipher suite is een combinatie van een bulk cipher (zoals AES), een kex-algoritme (zoals DH), een authenticatiemechanisme (zoals RSA) en een HMAC (zoals SHA-1 of SHA-2)

Bjornmeijer935
@Plopeye • 14 oktober 2015 09:22

+1

SHA1/2 hashing word gebruikt in combinatie met ciphers, in de comment van mij komt dit misschien over als of ik zeg dat SHA een ciphers is dat is niet wat ik bedoelde.

netdata
@Bjornmeijer935 • 13 oktober 2015 22:57

+1

Tenzij ik het niet goed door heb gaat het eerder over de SHA1 signature van de (Sub)CA waardoor zoals gezegd een collision kan bestaan tijdens de validate van de berekende SHA1 met de SHA1 uit de signature
Dit heeft dus niets te maken met cipher suites...

Armin
@netdata • 14 oktober 2015 20:40

+1

Inderdaad.

SHA1 wordt gebruikt voor zowel authenticatie (certifciaat) én als data verifciatie (hashing). De onveiligheid zit hem in gebruik als authentciatie. Als data verifciatie algorithme (HMAC) is het nog steeds veilig. Dat geldt bijvoorbeeld ook voor het nog oudere MD5.

Dus waar het zwak is, is als middel om te kijken of de server met wie je praat ook echt de server is met wie je wil praten. Ofwel of ING.nl ook echt de ING bank is. Of om dat Windows Update pakketje te controleren, dat het ook echt een van Microsoft afkomstige update is en geen malware.

Maar het wordt ook als data verifiatie gebruikt. Ofwel om te kijken of er coorruptie optrad door of transmissieproblemen of omdat iemand onderweg met zijn 'digitale handjes' aan een paketje gemorreld heeft.

Het heeft dus inderdaad niets met cipher suites te maken.

geenstijl
@netdata • 13 oktober 2015 21:27

+1

Zou het kunnen dat ze gewoon frequent hun certificaten vernieuwen, waardoor deze tussenperiode kleiner is dan de tijd die nu nog nodig is on te kraken?
(vraag, geen veronderstelling)
Ook veel overheidsorganisaties in ons land gebruiken nog sha1.

[Reactie gewijzigd door geenstijl op 13 oktober 2015 21:28]

robvanwijk
@geenstijl • 14 oktober 2015 03:25

+2

> Zou het kunnen dat ze gewoon frequent hun certificaten vernieuwen, waardoor deze tussenperiode kleiner is dan de tijd die nu nog nodig is on te kraken?
> (vraag, geen veronderstelling)

Nee, want het belangrijkste onderdeel van het onderzoek (lees ook het vorige artikel) is dat er nu een stap geparallelliseerd is, waarvan werd aangenomen dat dat niet goed kon. Dat maakt niet alleen het inzetten van GPUs (ipv CPUs) mogelijk, het betekent ook dat de conclusie **niet** is "kraken kan in een paar maanden", maar "*met een budget van 100.000 euro* kan kraken in een paar maanden". Ik weet niet hoe goed het precies schaalt, maar de volgende regel uit het vorige artikel

> "Met 512 grafische kaarten is een volledige aanval in enkele maanden uit te voeren, bij 1000 kaarten daalt dat tot enkele weken"

klinkt alsof je met twee keer de investering (bijna) twee keer de snelheid haalt. Als budget niet echt een punt is (bijvoorbeeld omdat je een niet-zo-frisse overheid bent die erg graag zijn burgers wil bespioneren), dan gooi je er een bak geld tegenaan en dan kan het nog veel sneller dan die paar maanden; die termijn is **geen** magische grens waar je nog steeds niet onder kunt duiken!

[Reactie gewijzigd door robvanwijk op 14 oktober 2015 03:26]

WhiteDog
@netdata • 13 oktober 2015 21:25

+1

Heeft dat niet te maken met compatibiliteit? Kan me voorstellen dat er een aantal oudere clients en browsers zijn die niet eens met sha2 overweg kunnen.

Tombastic
@WhiteDog • 13 oktober 2015 21:27

+1

Klopt inderdaad, in Chrome, Firefox of IE browser zal het gewoon werken met AES encryptie. Dus dit is opzich veilig genoeg voorlopig. Als het certificaat volledig sha1 zou zijn, dan zou het niet eens moeten werken in Chrome. (of duidelijk aangegeven)

[Reactie gewijzigd door Tombastic op 13 oktober 2015 21:27]

Sloerie
@Tombastic • 13 oktober 2015 22:31

+2

Dit heeft niets met AES of andere synchrone cryptografie te maken.

Doordat de mogelijkheid op collisions groter word kan iemand een ander certificaat maken met dezelfde 'hash' als diegene die verwacht word en zodoende de verbinding met een ander dan het originele certificaat opzetten.

Dit komt doordat men niet het certifiaat ondertekend maar de sha-1 digest (hash) daarvan. Aangezien deze collisions kan hebben (en die binnen enkele weken tot maanden gevonden kunnen worden) is het mogelijk een vals certificaat te maken en op te geven dat lijkt op het originele en zodoende alsnog voor te doen als het originele certificaat. Jij hebt echter de private key die bij dat certificaat hoort en kan dan mooi de verbinding opzetten zonder dat de ander jouw identiteit (correct) kan vaststellen.
Dit maakt bijvoorbeeld man-in-the-middle attacks mogelijk net als fishing sites met certificaten die echt lijken.

[Reactie gewijzigd door Sloerie op 13 oktober 2015 22:35]

N8w8
@Sloerie • 14 oktober 2015 00:22

+2

Bij een certificaat, kan je misschien wel (binnenkort makkelijk) data genereren met dezelfde SHA1 als dat certificaat.
Maar dan ben je er nog lang niet.
Die colliding data moet dan ook daadwerkelijk een geldig SSL certificaat zijn.
En daarbovenop; de domeinnamen e.d. in dat valse certificaat, moeten dan ook daadwerkelijk onder jouw controle staan.
Anders kan je er toch helemaal niks mee.
Dus dat lijkt me enorm veel stappen verder.

Dus ja, makkelijk collisions vinden is geen goede zaak en een sein dat het tijd wordt andere hashes te gaan gebruiken voor SSL certificaten.
Maar het is ook weer niet meteen armageddon.
Voor andere toepassingen (dan certificaten) die SHA1 gebruiken ligt dat wellicht anders, maar dat moet je per geval bekijken.

robb_nl
@N8w8 • 14 oktober 2015 08:40

+1

Ik begon al te twijfelen aan de (selfsigned) certificaten die openvpn gebruikt. Default hebben deze ook een sh1 hash. Je kan dit wel veranderen, maar bijvoorbeeld in de info voor pfsense staat expliciet dat de default aangeraden wordt.
Dat dit niet direct betekent dat je netwerk gecompromiteerd is, is dan wel enigzins geruststellend.

Tombastic
@Sloerie • 14 oktober 2015 07:26

+1

Los van dat het certificaat inderdaad onveilig is, zal dit geen impact hebben op de directe verbinding.

Bjornmeijer935
@WhiteDog • 13 oktober 2015 21:50

+1

De enige browser die ik me kan voorstellen die er niet mee kan werken is IE6. Verder zal iedere browser het ondersteunen dus er is geen enkele reden om niet sha2 te gebruiken. Wat betreft clients dit geld voor android 2.3 en Windows XP en Server 2003.

alt-92
@Bjornmeijer935 • 14 oktober 2015 12:11

+1

Het gaat niet alleen om browsers, maar om alle applicaties die TLS ondersteuning gebruiken om dataverkeer te versleutelen.
Dus ook de apps op je telefoon, maar eveneens je mailclient, je IM, je VPN client, ga zo maar door.
Als je Lync 2010 bijvoorbeeld in een bedrijfsomgeving hebt ben je nog deels afhankelijk van Sha1.

Bjornmeijer935
@alt-92 • 14 oktober 2015 12:39

+1

Er zullen genoeg applicaties aanwezig zijn die het nog niet ondersteunen, ik vind dit wel een kwalijk iets want SHA2 komt al uit 2005 het is niet iets nieuws sterker nog SHA3 zal ook niet lang meer op zich laten wachten. De developers van die applicaties hebben meer dan 10 jaar de tijd gehad om SHA2 support te integreren.
Uiteraard zijn ook de bedrijven die de software gebruiken verantwoordelijk voor het up-to-date houden en zo nodig dus aanschaf en testen van van nieuwere versies van de software.

alt-92
@Bjornmeijer935 • 14 oktober 2015 18:50

+1

10 jaar geleden was SHA2 een 'dure' aangelegenheid.
Je betaalde extra aan een CA, bijvoorbeeld.
CA's en hun subordinates signed alles nog met SHA1 op dat moment, met een levensduur van 10 jaar of meer.
Kijk maar eens naar de validity period van je gemiddelde (intermediate) CA.

Daarnaast was SHA2 een intensievere berekening (dus duurder in CPU cycles). Dat is voor één client niet echt een issue, maar voor serverside wel een behoorlijke impact.

Nog los van de complexiteit die 'even' SHA2 inbakken betekent.
Meeste ISV's doen dat in 'next version' maar jij weet net zo goed dat dat een utopisch wereldbeeld is om te verwachten dat dat wel effe kan.

[Reactie gewijzigd door alt-92 op 14 oktober 2015 18:54]

leuk_he
@Bjornmeijer935 • 13 oktober 2015 22:25

+1

Internet explorer 6 op xp sp3 ondersteund het. Ik vind het feit dat sommige grote enterpise klanten het nog niet zouden ondersteunen dus wel erg vaag.
Grote enterprise klanten kunnen immers hun eigen root certificaat uitrollen naar hun eigen stations.

Soldaatje
@netdata • 13 oktober 2015 22:19

+1

Die twee sites moeten dus voor het eind van het jaar bij de verlenging een SHA-2 certificaat regelen, anders zullen de browsers een waarschuwing geven.
En alle andere sites die nog SHA-1 gebruiken ook.
De reden van verlenging voor een jaar van SHA-1 was dat deze bedrijven naar hun zeggen nog duizenden certificaten gebruiken, die ze niet allemaal voor het einde van het jaar kunnen vervangen. Dus ze moeten daar even snel aan de bak, anders zal er wellicht het een en ander niet meer werken na de jaarwisseling.

Corteztm3
@netdata • 13 oktober 2015 23:04

+1

Cloudflare is wel bezig, zoals te lezen op hun blog, met SHA-256:
https://blog.cloudflare.com/test-all-the-things-ipv6-http2-sha-2/

Je kunt zelfs cloudflare al gebruiken met hun sha-256 certificates:
https://http2.cloudflare.com/

Verder geeft cloudflare ook een verklaring waarom zij nog gebruik maken van sha-1:
https://blog.cloudflare.c...e-and-sha-1-certificates/

[Reactie gewijzigd door Corteztm3 op 13 oktober 2015 23:33]

alexmeijer
14 oktober 2015 08:07

+1

Je kan toch gewoon 2x sha1 doen als beveiliging? Lijkt me niet zo makkelijk te kraken want als je er eentje kraakt blijft er nog wat anders random over. Of sha1(sha256(data)) etc?

R4gnax

@alexmeijer • 14 oktober 2015 09:15

+1

> Je kan toch gewoon 2x sha1 doen als beveiliging?

Dat is niet hoe hashing functies werken.
Er bestaat een zeer reeële kans dat het onzorgvuldig dubbel draaien van een hashing functie zowel leidt tot een algeheel verlies in entropie als tot een herkenbare relatie tussen in- en uitvoer die misbruikt zou kunnen worden.

CAPSLOCK2000
@alexmeijer • 14 oktober 2015 15:01

+1

> Je kan toch gewoon 2x sha1 doen als beveiliging? Lijkt me niet zo makkelijk te kraken want als je er eentje kraakt blijft er nog wat anders random over. Of sha1(sha256(data)) etc?

Je mag niet aannemen dat het veiliger is om het twee keer te doen. Het kan, maar dat hoeft niet, het zou zelfs minder veilig kunnen zijn. Alle onderzoek richt zicht zich op enkel SHA-1, over de veiligheid van dubbel SHA-1 valt niet zo veel te zeggen.

Je hebt er ook niet zo veel aan; je moet nog steeds de code van alle applicaties aanpassen. Als je dan toch bezig bent kun je het maar beter goed doen. Dat is nauwelijks meer werk en geeft een stuk meer zekerheid.

a fly
13 oktober 2015 23:48

+1

Waarom wordt er eigenlijk vertrouwd op één hashing algoritme voor certificaten? Gezien er altijd potentieel zwakheden in zitten, lijkt het mij veel sterker om 3 of meer algoritmes te gebruiken. Een colission op 3 of meer algoritmes krijgen is bijzonder veel moeilijker dan op 1.

leuk_he
@a fly • 14 oktober 2015 16:51

+1

Het hashing algoritme zelf gebruikt onderwater al verschillende stappen, die ook nog eens herhaalt worden. Maar ze moeten ook nog eens redelijk snel zijn op een CPU die relevant is. Zomaar de boel 3x vertragen, waarbij je niet kunt aantonen dat het 3x zo veilig is is niet een goede practice.

yPop
13 oktober 2015 21:14

+1

Net dit weekend mijn certificaten vervangen, Apple apps onder IOS 9 accepteerden mijn API niet meer.

mrcage
13 oktober 2015 21:25

+1

Dit is niet zo gek hoor. Certificaten worden vaak gebruikt voor externe connecties. Dit is aardig wat werk om het allemaal goed af te stemmen met de andere partij. Het overzetten is inderdaad zo gebeurd, maar zo werkt de wereld niet.

Tmonster94
13 oktober 2015 22:40

+1

Ik hoop dat Spring Security dan ook snel sha-256 gaat ondersteunen voor certificaten van externe bronnen, een link met een active directory leggen kan momenteel nog niet via sha 256, terwijl Spring en Spring Security momenteel erg veel worden gebruikt voor backend server applicaties.

MonotoneJeroen
13 oktober 2015 23:28

+1

Ik snap dat sommige bedrijven het versnelde uitfaseren van SHA-1 wat ongemakkelijk zit, maar het was al een tijdje verwacht dat SHA-1 langzamerhand vervangen word door SHA-2.

Zidane007nl
13 oktober 2015 22:02

0

Ik snap het niet dat Symantec en Microsoft achter verlenging stonden. Het is al 2 jaar bekend dat SHA-1 niet meer veilig is en het zal niet meer lang duren voordat een aanval betaalbaar is.

[Reactie gewijzigd door Zidane007nl op 13 oktober 2015 22:34]

CAPSLOCK2000
@Zidane007nl • 14 oktober 2015 15:08

+1

> Ik snap het niet dat Symantec en Microsoft achter verlenging stonden. Het is al 2 jaar bekend dat SHA-1 niet meer veilig is en het zal niet meer lang duren voordat een aanval betaalbaar is.

Die bedrijven krijgen veel vragen en klachten en zullen heel wat last hebben van deze overgang. Applicaties gaan op een onduidelijke manier stuk en mensen geven Microsoft de schuld. Als ze nog steeds met IE6 moeten werken hebben ze daar zelfs deels gelijk in. Nu wil MS zelf ook niks meer met IE6 te maken hebben maar de realiteit is dat het nog steeds wordt gebruikt.
Ik kan me dus wel voorstellen dat MS het liever nog een jaartje uitstelt, dat spaart een hoop werk voor de helpdesk.

Symantec moest ik wat langer over nadenken. Ik heb geen bevredigend antwoord. De eenvoudigste verklaring is dat Symantec nog oude troep in gebruik heeft bij klanten die ze niet willen vervangen.
De ingewikkelde verklaring die ik heb verzonnen is dat Symantec veiligheid verkoopt. Symantec wil misschien niet dat mensen te zien krijgen over onveilige websites. Mensen zouden kunnen denken dat Symantec z'n werk niet goed doet

Armin
@Zidane007nl • 14 oktober 2015 20:46

+1

SHA1 is niet onveilig. Het is echter niet zo sterk meer als je zou willen. Vandaar dat men het uitfaseerd.

Echter er zijn heel veel bedrijven die er moeite mee hebben. Dan is de vraag moet je het per 1-1-2016 doen of per 31-12-2016. Uiteindelijk heb je er niets aan als talloze servers en applicaties ermee stoppen. Zoals het er nu uitziet gaan veel bedrijven het niet halen.

Security is niet iets wat in een ivoren toren gaat of het hoogste goed is. Uiteindelijk is het een middel. Het idee was dat omdat veel bedrijven niet klaar zijn, één jaar extra uitstel te verlenen. Uiteraard is dat jammer, maar het zijn niet enkel de kleine ICT 'beunhazen' die nog niet klaar zijn. Omdat er geen direct gevaar was, was dat idee zo gek nog niet.

Echter het nieuwe onderzoek geeft aan dat de marge van veiligheid wlelicht kleiner is dan gedacht, en dan moeten we maar accepteren dat per 1-1-2016 een flink aantal servers en applicaties 'storingen' gaan ondervinden.

Waarschijnlijk overigens niet direct per 1-1-2016, maar waarschijnlijk per de eerste Microsoft Patch Tuesday, Chrome update, etc na 1-1-2016.

ONiel
13 oktober 2015 22:23

0

Vindt ik persoonlijk niet slecht.
Veiligheidsnormen moeten streng zijn, anders zijn ze geen 'garantie' voor veiligheid meer. En inderdaad was SHA-1 al even bekend als relatief onveilig.

Wel even een vraag, SHA-2 (256, 512,...) zijn vrij hard gebaseerd op SHA-1, zijn deze dan ook nog veilig? En als je even compatibiliteit wegdenkt, waarom zouden mensen dan deze nieuwere versie niet gebruiken, als 'ie veiliger is?

bkor
@ONiel • 13 oktober 2015 22:27

+1

SHA 2 lijkt juist totaal niet op SHA 1. D'r was wel iets anders met SHA-512, ik gebruik zelf standaard SHA-256 voor wanneer ik een hash nodig heb.

Ablaze
@ONiel • 14 oktober 2015 23:15

+1

Omdat alle certificaten dan omgezet moeten worden en bestaande softwarepakketten/servers die hiervan gebruik maken een upgrade moet krijgen.
Als je een paar certificaten en softwarepakketten/servers hebt is dat goed te doen, als je er een paar duizend hebt wat minder.

Daarnaast zijn er logge kantoor- en industriële toepassingen die soms ook nog als geheel gecertificeerd kunnen zijn voor bepaale toepassingen, waarbij een vervandering aan de veiligheidskant tot enorm veel werk kan leiden.

Ook zijn er embedded apparaten die helemaal geen OS update kunnen krijgen en daardoor de nieuwere technieken niet kunnen toepassen.

Op dit item kan niet meer gereageerd worden.

AIVD: terroristen hebben te weinig capaciteiten om te hacken
App Store van Apple kampt met storing - update