Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Schakel SSL 2.0 uit en upgrade OpenSSL

Met DROWN-aanvalstechnieken kan aanvaller TLS-beveiliging doorbreken

Factsheet FS-2016-03 | versie 1.0 | 2 maart 2016

Op 1 maart heeft een groep onderzoekers de DROWN-aanvalstechnieken voor TLS gepresenteerd. Met DROWN maakt een aanvaller misbruik van servers die nog SSL 2.0 ondersteunen. Servers die een kwetsbare versie van OpenSSL gebruiken zijn op dezelfde manier te misbruiken, ongeacht of ze SSL 2.0 ondersteunen. Een aanvaller die met TLS beveiligd netwerkverkeer weet te onderscheppen, kan dit verkeer proberen te kraken met behulp van de kwetsbare server. Hij kan daardoor het verkeer inzien.

Het NCSC adviseert om TLS altijd te configureren op basis van de ICT-beveiligingsrichtlijnen voor Transport Layer Security. Schakel daarom SSL 2.0 uit, installeer de recentste updates van OpenSSL en geef op servers de voorkeur aan cipher suites op basis van forward secrecy.

Doelgroep

IT-beheerders, informatiebeveiligers, IT-managers

Aan deze factsheet heeft bijgedragen:

Nationaal Bureau Verbindingsbeveiliging

Achtergrond

Transport Layer Security (TLS) is het meestgebruikte protocol voor het beveiligen van internetverbindingen. Met behulp van TLS kunnen een client en een server een cryptografisch beveiligde tunnel opzetten. Na het opzetten van de tunnel kunnen client en server veilig met elkaar communiceren.

SSL 2.0 is een heel oude versie van TLS. Het is al lang bekend dat SSL 2.0 kwetsbaarheden bevat. Sommige mensen gingen er echter vanuit dat het aanbieden van SSL 2.0 als optie geen aanvullend risico met zich meebracht. Als gevolg daarvan zijn er nog veel servers die SSL 2.0 aanbieden, naast nieuwere veiligere opties.

OpenSSL is een populaire programmeerbibliotheek voor het implementeren van de functionaliteit van TLS. TLS is een complex protocol. De meeste applicaties maken daarom gebruik van een programmeerbibliotheek om het protocol te implementeren. Vooral serversoftware gebruikt daarvoor vaak OpenSSL.

Wat is er aan de hand?

Op 1 maart 2016 heeft een groep onderzoekers een aantal nieuwe aanvalstechnieken voor TLS gepresenteerd.[1] Ze hebben deze technieken DROWN genoemd. DROWN staat voor 'Decrypting RSA with Obsolete and Weakened eNcryption'.

Met DROWN maakt een aanvaller misbruik van servers die nog SSL 2.0 ondersteunen. Dit komt nog relatief vaak voor, bijvoorbeeld bij mailservers. Het maakt daarbij niet uit welke programmeerbibliotheek de server gebruikt.

Servers die een kwetsbare versie van OpenSSL gebruiken zijn op dezelfde manier te misbruiken. Daarbij maakt het niet uit of de beheerder SSL 2.0 heeft uitgeschakeld in de configuratie van OpenSSL. Deze kwetsbaarheid in OpenSSL is opgelost op 28 januari 2016.[2] Deze versies zijn niet meer kwetsbaar, indien SSL 2.0 in de configuratie is uitgeschakeld.

Een aanvaller die met TLS beveiligd netwerkverkeer weet te onderscheppen, kan dit verkeer proberen te kraken met behulp van de kwetsbare server. Het is daarvoor nodig dat de kwetsbare server en de server die het TLS-verkeer uitwisselt, dezelfde geheime sleutel (private key) gebruiken voor het TLS-certificaat. In het bijzonder kan het dus om dezelfde server gaan. Het maakt daarbij niet uit met welke versie van TLS het onderschepte TLS-verkeer is beschermd.

De onderzoekers hebben hun programmeercode voor het uitvoeren van DROWN nog niet gepubliceerd. Dat maakt het uitvoeren van de aanval aanzienlijk moeilijker. Alleen een aanvaller met veel kennis van zaken zal in staat zijn op basis van alleen het onderzoeksrapport de aanval uit te voeren. De onderzoekers hebben aangegeven de code voorlopig nog niet vrij te zullen geven.

Wat kan er gebeuren?

Een aanvaller die DROWN gebruikt, onderschept eerst ongeveer duizend TLS-sessies. Deze sessies moeten allemaal met servers zijn die dezelfde geheime sleutel gebruiken als de kwetsbare server. Ook moeten al deze sessies geen gebruik maken van 'forward secrecy'. Vervolgens gebruikt hij gegevens uit de onderschepte sessies om bij de kwetsbare server enkele tienduizenden verbindingen op te zetten. Door het slim manipuleren van de kwetsbare server weet de aanvaller de sessiesleutel van gemiddeld een van de TLS-sessies te achterhalen.[3]

Met behulp van de achterhaalde sessiesleutel kan de aanvaller een van de duizend onderschepte TLS-sessies ontsleutelen. Hij kan dan beschikken over de volledige inhoud van deze sessie. Gevoelige gegevens die met TLS beveiligd hadden moeten zijn, zijn voor de aanvaller dan in te zien. Het is van tevoren voor de aanvaller niet te bepalen welke van de duizend sessies hij zal kraken. Ook kan hij niet door zich verder in te spannen meer van die sessies kraken.

Het uitvoeren van de aanval kost volgens de onderzoekers ongeveer € 400 en acht uur rekentijd. Dat zijn de kosten voor het kraken van gemiddeld een van de duizend TLS-sessies.

Special DROWN

Een speciale variant van de aanval, 'special DROWN', is veel eenvoudiger en tegen lagere kosten uit te voeren. De aanvaller kan dan ook verbindingen met forward secrecy kraken, of zich voordoen als de kwetsbare server. Deze variant vereist echter dat de kwetsbare server een verouderde versie van OpenSSL gebruikt. Versies vanaf 1.0.2a, 1.0.1m, 1.0.0r en 0.9.8zf zijn niet kwetsbaar. Updates naar deze versies zijn uitgebracht op 19 maart 2015.[4]

Het kraken van een op de duizend sessies klinkt niet erg schokkend, maar er zijn genoeg scenario's waarin elke sessie gevoelig is. Als er bijvoorbeeld inloggegevens worden verstuurd, maakt het voor de aanvaller niet uit welke sessie hij van een gebruiker weet te kraken. Elke sessie bevat immers dezelfde inloggegevens.

Wat adviseert het NCSC?

Het NCSC adviseert om TLS altijd te configureren op basis van de ICT-beveiligingsrichtlijnen voor Transport Layer Security[5]. Schakel daarom SSL 2.0 uit, installeer de recentste updates van OpenSSL[6] en geef op servers de voorkeur aan cipher suites op basis van forward secrecy.

Het uitschakelen van SSL 2.0 op servers zou geen negatieve gevolgen moeten hebben voor de werking van ICT-systemen.

[1] https://drownattack.com/
[2] CVE-2015-3197, http://openssl.org/news/secadv/20160128.txt
[3] Het aantal sessiesleutels dat de aanvaller achterhaalt, hangt af van het aantal onderschepte sessies. Bij duizend sessies is het verwachte aantal achterhaalde sessiesleutels één.
[4] CVE-2015-0703, http://openssl.org/news/secadv/20160301.txt
[5] Zie https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html.
[6] Strikt genomen zijn de kwetsbaarheden die hier worden besproken, al opgelost in de voorlaatste versie van OpenSSL (verschenen op 28 januari 2016). Het is desondanks altijd een goed idee te upgraden naar de recentste versie.

SSL 2.0 is al zo lang verouderd dat er nauwelijks nog systemen bestaan die het vereisen. Wel kan het in sommige gevallen zo zijn dat de optie om SSL 2.0 uit te schakelen ontbreekt. Zie voor alternatieve maatregelen het kader 'Veilig door netwerkdetectie en firewalling'.

Het updaten van OpenSSL naar de recentste versie is mogelijk voor alle servers waarvan het besturingssysteem nog onderhouden wordt. Versies vanaf 1.0.2f en 1.0.1r zijn niet meer kwetsbaar. Sommige makers van besturingssystemen bieden nog een oude versie, maar 'backporten' de beveiligingsupdates naar die versie. Op sommige apparaten is het niet mogelijk om de beveiligingsupdates te installeren. Zie voor alternatieve maatregelen het kader 'Veilig door netwerkdetectie en firewalling'.

Veilig door netwerkdetectie en firewalling

Met behulp van netwerkdetectie kan de DROWN-aanvalstechniek gedetecteerd worden. De techniek vereist namelijk enkele tienduizenden verbindingen op basis van SSL 2.0 naar de kwetsbare server. Detecteert u veel verbindingen op basis van SSL 2.0 in uw netwerkverkeer, dan kan dat wijzen op een DROWN-aanval.

DROWN-aanvallen zijn te voorkomen door al het netwerkverkeer op basis van SSL 2.0 naar eventueel kwetsbare servers te blokkeren. Legitiem SSL 2.0-verkeer is immers buitengewoon schaars. Dit kan echter een beheerintensieve maatregel zijn. Gebruik dit daarom alleen als alternatief voor reguliere maatregelen (uitschakelen van SSL 2.0 en updaten van OpenSSL).

Voorkom het breed hergebruik van geheime sleutels tussen servers. Is een server kwetsbaar voor de DROWN-aanvalstechniek, dan zijn alle servers die dezelfde geheime sleutel gebruiken dat ook. Zorg in het bijzonder dat derde partijen die over geheime sleutels van uw certificaten beschikken, niet dezelfde sleutels gebruiken als u gebruikt op uw eigen systemen. Over de configuratie van de servers van deze derde partijen heeft u immers maar beperkt invloed. Voorbeelden van zulke derde partijen zijn aanbieders van anti-DDoS-dienstverlening of contentdeliverynetwerken (CDN's) voor websites.

Het is niet nodig om naar aanleiding van de DROWN-aanvalstechniek over te gaan tot de vervanging van TLS-certificaten. De aanvaller krijgt immers niet de beschikking over de geheime sleutel van het certificaat.

Het is niet mogelijk om mitigerende maatregelen te treffen aan de zijde van de client in een TLS-verbinding. De kwetsbaarheden doen zich volledig voor aan de kant van de server.

Handelingsperspectief

- Inventariseer welke servers in uw organisatie TLS aanbieden. Groepeer deze servers op basis van hergebruik van geheime sleutels. Delen server A en server B een geheime sleutel, dan vallen server A en B in een groep. Betrek ook servers van externe leveranciers bij deze inventarisatie als ze geheime sleutels delen met systemen die u zelf beheert.
- Pas voor elke groep servers het hoofdadvies toe: schakel op alle servers SSL 2.0 uit en upgrade OpenSSL naar een versie van na 28 januari 2016.[7]
- Is het toepassen van het hoofdadvies voor de groep servers geen optie, stel uw firewall dan in om SSL 2.0-verkeer te blokkeren naar alle servers in de groep waarvoor u het hoofdadvies niet toepast.

[7] Zie ook https://www.ncsc.nl/dienstverlening/response-op-dreigingen-en-incidenten/beveiligingsadviezen/NCSC-2016-0196+1.01+Kwetsbaarheid+ontdekt+in+SSL+2.0.html.

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

FS-2016-03 | versie 1.0 | 2 maart 2016