Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Heartbleed: Ernstige kwetsbaarheid in OpenSSL

Upgrade OpenSSL en vervang certificaten

Factsheet FS-2014-02
versie 1.1 | 11 april 2014

Op 7 april 2014 is de Heartbleed-kwetsbaarheid gepubliceerd[1]. Dit is een kwetsbaarheid in programmeerbibliotheek OpenSSL. Een aanvaller kan geheime sleutels en certificaten achterhalen van een kwetsbare server of ander apparaat. Ook andere gevoelige informatie zoals wachtwoorden en klantgegevens kan worden achterhaald.

Met de geheime sleutels van certificaten kan de aanvaller informatie achterhalen uit versleutelde verbindingen die worden gebruikt voor bijvoorbeeld websites, e-mail en VPN.

Deze ernstige kwetsbaarheid kan worden weggenomen door de server of het andere apparaat te upgraden naar een versie van OpenSSL die niet kwetsbaar is. Daarnaast is het raadzaam certificaten en de bijbehorende geheime sleutels te vervangen als deze op een kwetsbare server of ander apparaat gebruikt zijn.

De belangrijkste feiten:

- Er is een kwetsbaarheid gevonden in OpenSSL waardoor een aanvaller van buitenaf het interne geheugen uit kan lezen van de applicatie die OpenSSL gebruikt.
- In het interne geheugen van de applicatie staan geheime sleutels van certificaten voor SSL/TLS opgeslagen. Ook andere vertrouwelijke gegevens uit de applicatie kunnen zo bereikbaar zijn.
- Met behulp van de geheime sleutels kan een aanvaller verkeer van met SSL/TLS beveiligde verbindingen ontsleutelen.
- Het NCSC adviseert om kwetsbare versies van OpenSSL te upgraden naar een versie die niet kwetsbaar is. Vervolgens adviseert het NCSC de geheime sleutels en certificaten te vervangen die via kwetsbare apparaten te bereiken waren.

Achtergrond

OpenSSL is een populaire programmeerbibliotheek voor het implementeren van het SSL/TLS-protocol. Veel webservers, VPN-servers, mailservers en andere applicaties maken gebruik van OpenSSL om beveiligde verbindingen op te zetten. Ook andere apparaten kunnen OpenSSL gebruiken. Voorbeelden zijn appliances, routers, WiFi-accesspoints en sommige applicaties op clientsystemen. De meeste beveiligde verbindingen via het internet werken op basis van SSL/TLS. Een bekend voorbeeld is het HTTPS-protocol om een beveiligde verbinding met een webserver op te zetten.

Om een verbinding te beveiligen met SSL/TLS, is een certificaat nodig met een geheime sleutel. De geheime sleutel staat op de server of het andere apparaat opgeslagen, maar kan normaliter niet worden opgevraagd. Terwijl de server of het apparaat actief is, staat de geheime sleutel ook in het interne geheugen van de server of het andere apparaat opgeslagen.

Wat is er aan de hand?

Er is een kwetsbaarheid gevonden in OpenSSL waardoor een aanvaller van buitenaf het interne geheugen uit kan lezen van de applicatie die OpenSSL gebruikt. In het interne geheugen staat allerlei vertrouwelijke informatie opgeslagen, waaronder de geheime sleutels van certificaten. De kwetsbaarheid ontstaat door een programmeerfout in de heartbeat-functionaliteit: de ontdekkers hebben de kwetsbaarheid daarom Heartbleed genoemd.

[1] Zie http://heartbleed.com.

De heartbeat-functionaliteit is een optioneel onderdeel van de SSL/TLS-standaard[2]. Alleen apparaten die de heartbeat-functionaliteit ondersteunen, zijn kwetsbaar voor deze aanval[3].

De kwetsbaarheid is geen onderdeel van het SSL/TLS-protocol, maar ontstaat door een programmeerfout in de OpenSSL-code. Andere implementaties dan OpenSSL zijn daarom niet kwetsbaar. De kwetsbare code is sinds maart 2012 onderdeel van OpenSSL: aanvallers hebben dus lang de tijd gehad om misbruik te maken van deze kwetsbaarheid. Achteraf is het vrijwel onmogelijk om uit te sluiten dat een apparaat is aangevallen. Alleen uit analyse van het netwerkverkeer blijkt de aanval; in de logs op het apparaat is deze niet zichtbaar.

De ontwikkelaars van OpenSSL hebben de kwetsbaarheid gerepareerd in de recentste versie, 1.0.1g[4]. Softwareleveranciers die OpenSSL met hun software meeleveren, zoals Linux-distributies, zullen op basis hiervan updates uitbrengen[5]. Dit geldt ook voor de firmware van andere apparaten die OpenSSL toepassen.

Sinds de kwetsbaarheid is gepubliceerd, is er code publiek beschikbaar gekomen om deze kwetsbaarheid te misbruiken. Deze code wordt inmiddels op grote schaal gebruikt om apparaten te testen of aan te vallen.

Hardware Security Modules

Soms staan de geheime sleutels van certificaten niet opgeslagen op de server, maar in een aparte hardwaremodule: een Hardware Security Module (HSM). Deze module voert de cryptografische berekeningen namens de server uit. De geheime sleutels blijven in de module en zijn nooit bereikbaar via de server.

Geheime sleutels van certificaten die alleen opgeslagen zijn in een HSM, zijn in principe niet bereikbaar voor een aanval via deze kwetsbaarheid. Wel kan er ander gevoelig materiaal buitgemaakt worden met deze aanval, zoals wachtwoorden, sessiesleutels en gevoelige (klant)gegevens.

Wat kan er gebeuren?

Een aanvaller kan een kwetsbaar apparaat op afstand benaderen en het interne geheugen van de applicatie die OpenSSL gebruikt uitlezen. Elke keer dat de aanvaller de aanval uitvoert, ontvangt hij een willekeurig blok van 64 KB aan gegevens uit het interne geheugen. Naast geheime sleutels van certificaten, bevat het interne geheugen nog meer gevoelige informatie.

- Bij een *webserver* kan een aanvaller beschikken over alle broncode van de webapplicaties, wachtwoorden van systemen en klanten, sessiesleutels, afgeschermde informatie uit de webapplicatie en andere gevoelige informatie die door de webserver verwerkt wordt.
- Bij een *mailserver* kan een aanvaller beschikken over de inhoud van alle e-mail die op dat moment verwerkt wordt, wachtwoorden van gebruikers en andere gevoelige informatie die door de mailserver verwerkt wordt.
- Bij een *VPN-server* kan een aanvaller beschikken over de informatie die op dat moment verzonden of ontvangen wordt en (afhankelijk van de configuratie) over inloggegevens van gebruikers. Daarnaast kan de aanvaller beschikken over andere gevoelige informatie die door de VPN-server verwerkt wordt.
- Ook bij *andere apparaten* kan een aanvaller beschikken over alle informatie die in het geheugen van het apparaat verwerkt wordt. Welke informatie dat is, hangt af van de functionaliteit van het apparaat.

Met de geheime sleutel van een certificaat kan een aanvaller verkeer ontsleutelen dat verzonden is via de beveiligde verbinding. Een aanvaller die kan optreden als man-in-the-middle, kan het verkeer onderscheppen, ontsleutelen en aanpassen. Een aanvaller die eerder versleuteld verkeer van de beveiligde verbinding heeft opgeslagen, kan later de bijbehorende sleutel gebruiken om dit verkeer te ontsleutelen.

Wat adviseert het NCSC?

Het NCSC adviseert om uw kwetsbare servers en andere apparaten op korte termijn te upgraden naar een versie van OpenSSL die niet kwetsbaar is. Krijgt u OpenSSL meegeleverd met een apparaat of met andere software, vraag uw leverancier dan wanneer een versie beschikbaar zal komen die een niet-kwetsbare versie van OpenSSL ondersteunt.

Is upgraden geen optie, dan kunt u ook besluiten de heartbeat-functionaliteit uit te schakelen in OpenSSL. Daarvoor zult u zelf de OpenSSL-broncode moeten compileren zonder de heartbeat-functionaliteit. Het NCSC ontraadt dit op productiesystemen, vanwege de toegenomen beheerlast die samenhangt met het zelf compileren van broncode. Mocht u deze oplossing toch kiezen, dan kunt u instructies gebruiken die daarvoor door de ontwikkelaars van OpenSSL beschikbaar zijn gesteld[6].

Het NCSC adviseert verder om certificaten en geheime sleutels te vervangen die op kwetsbare apparaten hebben gestaan. Dit proces is drieledig: ten eerste moet u nieuwe geheime sleutels genereren. Ten tweede moet u nieuwe certificaten op basis van deze geheime sleutels verkrijgen van uw certificaatleverancier en deze installeren. Ten derde moet u de oude certificaten intrekken of in laten trekken. Uw certificaatleverancier kan u hiermee helpen.

[2] Zie https://tools.ietf.org/html/rfc6520 voor meer details over heartbeat.
[3] De heartbeat-functionaliteit is in OpenSSL standaard ingeschakeld.
[4] Bron: https://www.openssl.org/news/secadv_20140407.txt
[5] Zie http://www.kb.cert.org/vuls/id/720951 voor een overzicht van kwetsbare systemen.
[6] Zie https://www.openssl.org/news/secadv_20140407.txt voor de instructie om OpenSSL zonder heartbeat-functionaliteit te compileren.

Handelingsperspectief:

1. Inventariseer welke van uw servers en andere apparaten een kwetsbare versie van OpenSSL gebruiken[7].
2. Inventariseer welke geheime sleutels van certificaten worden gebruikt op een kwetsbare server of ander apparaat.
3. Upgrade alle apparaten met een kwetsbare versie van OpenSSL naar een versie die niet meer kwetsbaar is. Is upgraden niet mogelijk, compileer OpenSSL dan zonder ondersteuning voor de heartbeat-functionaliteit[8]. Herstart de applicaties die OpenSSL gebruiken.
4. Genereer nieuwe geheime sleutels en vraag nieuwe certificaten aan voor alle sleutels die mogelijk gecompromitteerd zijn (zie stap 2).
5. Vervang de mogelijk gecompromitteerde sleutels en certificaten door nieuwe exemplaren op servers en andere apparaten met een geüpgradede versie van OpenSSL. Plaats geen nieuwe sleutels en certificaten op apparaten zolang deze nog kwetsbaar zijn.
6. Laat uw certificaatleverancier de certificaten intrekken die u zojuist vervangen heeft.

In sommige gevallen biedt uw certificaatleverancier u de mogelijkheid uw certificaten te 'rekeyen'. Hierbij krijgt u het zelfde certificaat uitgereikt, maar dan gebaseerd op een nieuwe geheime sleutel. Dit is een goed en mogelijk goedkoper alternatief voor het aanvragen van nieuwe certificaten.

Ten slotte adviseert het NCSC om te inventariseren welke gegevens er mogelijk gelekt zijn via deze kwetsbaarheid, en wat de gevolgen daarvan zijn. Houd daarbij in gedachten dat de kwetsbaarheid al sinds maart 2012 bestaat, en pas begin april 2014 ontdekt en gerepareerd is. Gedurende deze periode was de recentste versie van OpenSSL steeds kwetsbaar. Betreft dit gegevens van uw klanten, overweeg dan om hen te informeren over de situatie en stappen die ze zelf kunnen nemen om fraude met hun gegevens te voorkomen, zoals het wijzigen van wachtwoorden.

Tot slot

Deze kwetsbaarheid vormt een groot risico voor de beveiliging van netwerkverkeer: het geheim blijven van de geheime sleutels van certificaten is een fundament van de vertrouwelijkheid van veel informatie. Verwerkt u gevoelige gegevens van welke aard dan ook, dan is het van het grootste belang dat u op korte termijn zorgt dat uw organisatie niet langer kwetsbaar is voor deze aanval, en dat u niet langer vertrouwt op geheime sleutels en certificaten die mogelijk gecompromitteerd zijn.

[7] Zie http://www.kb.cert.org/vuls/id/720951 voor een overzicht van kwetsbare systemen.
[8] Zie https://www.openssl.org/news/secadv_20140407.txt voor de instructie om OpenSSL zonder heartbeat-functionaliteit te compileren.

Uitgave van **Nationaal Cyber Security Centrum**

Verder hebben bijgedragen: **NBV, Schuberg Philis**
Turfmarkt 147 | 2511 DP Den Haag
Postbus 117 | 2501 CC Den Haag
www.ncsc.nl | info@ncsc.nl
T 070-888 75 55 | F 070-888 75 50
Publicatienr: FS-2014-02 1.1