Publicatie : Linux Magazine
Datum : 31 mrt 2016
cm2 : 718
Pagina : 50
Advertentiewaarde : € 4.125,00
Regio : Nederland
Frequentie : 6x per jaar
Oplage : 11.500

FOCUS OP VEILIGHEID

FOCUS OP VEILIGHEID

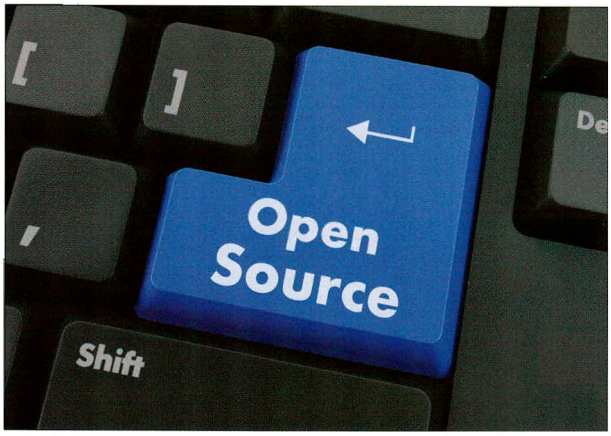
Juniper Networks ontdekte twee backdoors in zijn firewalls. En Nederland investeert een half miljoen euro in open source encryptieprojecten. Deze en andere beveiligingsnieuwties lees je in Focus op veiligheid. **Koen Vervloesem**

NEDERLAND INVESTEERT IN OPENSOURCE ENCRYPTIE

In december nam de Nederlandse Tweede Kamer een voorstel van D66 aan om een half miljoen euro te doneren aan open source encryptieprojecten. D66 wilde in het originele voorstel het bedrag aan OpenSSL schenken, terwijl het aangenomen voorstel dit breder trekt en naast OpenSSL ook LibreSSL en PolarSSL (tegenwoordig mbed TLS) als mogelijke begunstigden noemt. "Deze projecten," zo zegt het aangenomen voorstel, "draaien dikwijls grotendeels op vrijwilligers en de encryptiesoftware wordt in veel diensten toegepast, zoals web- en e-mailservers en mobiele apps en is daarmee van groot belang voor miljoenen mensen over de hele wereld." Het geld komt uit het potje voor ICT-beleid van het Ministerie van Economische Zaken. Het ministerie zal in samenspraak met deskundigen uit het veld projecten selecteren die cruciaal zijn voor de internationale internetinfrastructuur.

Nog interessanter dan het geld dat vrij komt, is de toelichting die de ministers van Veiligheid en Justitie en van Economische Zaken, respectievelijk Ard van der Steur en Henk Kamp, geven in een gezamenlijke brief aan de Tweede Kamer. Zij gaan daarin uitgebreid in op de tweeledigheid van encryptie: enerzijds het belang van vertrouwelijkheid en integriteit van communicatie voor de maatschappij en economie, en anderzijds de belemmering die encryptie biedt voor opsporings-, inlichtingen- en veiligheidsdiensten wanneer criminelen en terroristen ervan gebruikmaken. In de brief wijzen de ministers resoluut de 'oplossing' af die regelmatig door politici in binnen- en buitenland wordt voorgesteld, namelijk een backdoor in encryptiesoftware verplichten zodat de overheid versleutelde communicatie indien nodig kan ontcijferen. Hun conclusie: "Door bijvoorbeeld een technische ingang in een encryptieproduct te introduceren die het voor opsporingsinstanties mogelijk zou maken versleutelde bestanden in te zien, kunnen digitale systemen kwetsbaar worden voor bijvoorbeeld criminelen, terroristen en buitenlandse inlichtingendiensten. Dit zou onwenselijke gevolgen hebben voor de beveiliging van gecommuniceerde en opgeslagen informatie, en de integriteit van ICT-systemen, die in toenemende mate van belang zijn voor het functioneren van de samenleving." Ook andere beperkende wettelijke maatregelen over de ontwikkeling, beschikbaarheid en het gebruik van encryptie zijn volgens het kabinet niet wenselijk. Met het voorstel en het geld dat daarmee vrij komt, wil het kabinet dan ook encryptie helpen versterken in plaats van verzwakken.

http://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2016Z00009&did=2016D00015



HASHCAT EN OCLHASHCAT ZIJN OPENSOURCE

De populaire wachtwoordkrakers Hashcat (CPU-gebaseerd) en oclHashcat (GPGPU-gebaseerd) zijn door hun ontwikkelaars opensource gemaakt, onder de MIT-licentie. Een van de redenen was dat de ontwikkelaars nu meer externe library's kunnen integreren, bijvoorbeeld als die onder de restrictieve GPL zijn vrijgegeven. Een andere reden is dat nu native ondersteuning op OS X mogelijk wordt. Overigens worden de hashcat en oclHashcat projecten in de toekomst samengevoegd, iets wat ook door het open sourcen versneld mogelijk is.

https://hashcat.net/
https://hashcat.net/forum/thread-4880.html

Publicatie : Linux Magazine
Datum : 31 mrt 2016
cm2 : 718
Pagina : 50
Advertentiewaarde : € 4.125,00
Regio : Nederland
Frequentie : 6x per jaar
Oplage : 11.500

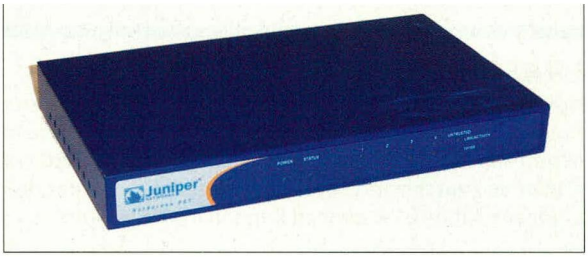
JUNIPER-FIREWALLS BEVATTEN BACKDOORS

Juniper Networks kondigde eind 2015 aan dat het twee backdoors in zijn propriëtaire besturingssysteem ScreenOS had gevonden dat op de Juniper NetScreen firewalls draait. Tijdens een interne code review vond het bedrijf namelijk "unauthorized code" die twee kwetsbaarheden introduceerde. ScreenOS is al minstens sinds 2012 kwetsbaar. De eerste kwetsbaarheid is een hard gecodeerd wachtwoord dat met elke gebruikersnaam werkt, waarmee onbevoegden op afstand via ssh of telnet administratieve toegang tot de firewalls krijgen. Fox-IT slaagde er in slechts zes uur in om op basis van de info in de patch van Juniper de ScreenOS-firmware te reverse-engineeren en daaruit het wachtwoord te achterhalen.

Met de tweede kwetsbaarheid is een aanvaller die VPN-verkeer kan monitoren in staat om het versleutelde netwerkverkeer te ontcijferen. ScreenOS maakt gebruik van Dual_EC_DRBG als pseudo-random number generator (PRNG), dat als parameters twee punten P en Q op een elliptische kromme heeft. De release van augustus 2012 introduceerde plots een andere Q, wat blijkbaar niet door Juniper was geautoriseerd. Diegene die Q speciaal gekozen heeft, kan de interne toestand van de PRNG afleiden. De sleutels voor de encryptie worden dan niet meer willekeurig gegenereerd, waardoor de aanvaller de hele encryptie van de VPN-verbinding kan kraken. De manier waarop dat gaat, werd al in 2007 beschreven door Niels Ferguson en Dan Shumow. Er waren toen vragen over de Q die in de officiële specificatie van Dual_EC_DRBG stond, omdat de NSA daar een hand in zou hebben. Juniper was zich daarvan bewust en had daarom een andere Q gekozen, maar had er geen rekening mee gehouden dat iemand anders wel eens een eigen Q in de code kon introduceren. ScreenOS gebruikte naast Dual_EC_DRBG ook een andere PRNG als extra beveiligingsmaatregel, ANSI X.9.31. Maar beveiligingsspecialist Willem Pinckaers ontdekte na de aankondiging van Juniper dat door een bug in ScreenOS ANSI X.9.31 volledig werd genegeerd...

Onmiddellijk waren er geruchten dat die backdoors van de NSA afkomstig zouden zijn. In 2013 bleek immers uit gelekte documenten dat de NSA door het FEEDTHROUGH-programma toegang had tot Juniper-firewalls. Maar de backdoor in de Dual_EC_DRBG-implementatie van Juniper zou ook wel eens van Juniper zelf kunnen zijn. Want zij hebben een eigen Q gebruikt en kunnen als die niet willekeurig gegenereerd is zelf alle VPN-verkeer door hun firewalls ontcijferen. Door de inherente zwakheid in Dual_EC_DRBG had Juniper het PRNG-algoritme eigenlijk al in 2013 moeten verwijderen. Of, wat cryptografieprofessor Matthew Green denkt, Juniper heeft de backdoor geïntroduceerd, dat wordt door een buitenlandse inlichtingendienst ontdekt en die introduceert zijn eigen Q, zodat ze eenvoudig misbruik kunnen maken van de bestaande backdoor. Wat alleen maar bewijst hoe onzinnig de voorstellen van politici in de VS en Groot-Brittannië zijn om de overheid een backdoor in encryptiesoftware te geven...

http://forums.juniper.net/t5/Security-Incident-Response/Important-Announcement-about-ScreenOS/ba-p/285554



TAILS 2.0

De Linux-distributie voor privacybescherming Tails heeft versie 2.0 uitgebracht. Het is de eerste versie gebaseerd op Debian Jessie (8), waardoor heel wat software een upgrade krijgt. Zo toont de desktop nu de GNOME Shell, zij het in Classic mode. Een nadeel van de overstap is wel dat Tails 2.0 niet meer de Windows-camouflagemodus heeft, omdat die niet naar GNOME Shell is geport. In die modus zag Tails eruit als Windows 8, waardoor je minder de aandacht trok als je de distributie op een publieke plaats gebruikte. Ook Claws Mail is verwijderd in Tails 2.0. De officiële mailclient in de distributie is sinds versie 1.8 Icedove, de Debian-rebranded versie van Mozilla Thunderbird.

https://tails.boum.org

EN VERDER

Door een bug in GRUB2 kan iemand die 28 keer op backspace duwt -wanneer de bootloader om een gebruikersnaam vraagt- de authenticatiestap omzeilen. De fout werd door de ontdekkers 'Back to 28' gedoopt. De webbrowser Google Chrome ondersteunt sinds dit jaar geen SHA-1 SSL-certificaten meer. Die beslissing komt als antwoord op recent onderzoek door wetenschappers van het CWI, Inria en NTU Singapore met als conclusie dat de kosten om SHA-1 te breken significant lager liggen dan eerder gedacht.

BlackBerry heeft een veilige Android-smartphone geïntroduceerd, de PRIV. De Electronic Frontier Foundation (EFF) introduceerde Panopticlick 2.0, de nieuwe versie van zijn fingerprinting website om te tonen hoe je op het web geïdentificeerd kunt worden aan de hand van je browser. Een Tsjechische start-up wil met de Turris Omnia een veilige router ontwikkelen, gebaseerd op open hardware en het OpenWRT-besturingssysteem. De Indiegogo-campagne voor crowdfunding was immens populair en bracht maar liefst vijf keer meer geld in het laatje dan nodig. En in het opensource CMS Joomla! werd een acht jaar oud kritiek beveiligingslek ontdekt, dat al actief werd misbruikt.