BLOG | Kim Tiedemann

EMNER *Internet Explorer, Offentlig it, Sikkerhedshuller, Webapplikationer*

Kan vi ikke snart blive fri for IE6

Af Kim Bjørn Tiedemann 15. oktober 2014 kl. 12:08

Google har på deres sikkerhedsblog (http://googleonlinesecurity.blogspot.dk/2014/10/this-poodle-bites-exploiting-ssl-30.html) beskrevet en sårbarhed i SSLv3, som er en ret effektiv måde at fiske secure cookie informationer ud af en sikret https forbindelse. SSLv3 er efterhånden 15 år gammel, men Google beskriver at den stadig er meget brugt.

Det skræmmende ved sårbarheden er, at næsten alle browsere understøtter SSLv3 og en angriber kan ved at manipulere med netværkstrafikken tvinge browser/server ned på SSLv3 i den såkaldte downgrade dance. Så hvis serveren understøtter SSLv3, så er man sårbar overfor angrebet.

Hvad med de offentlige sites?

Der findes et nemt online tool (http://poodlebleed.com/) til at checke, om en server understøtter SSLv3 og dermed om den er sårbar for PoodleBleed.

Her er en liste over offentlige sites, som pt. er sårbare:

- borger.dk
- jobnet.dk
- nemlog-in.dk
- skat.dk
- e-boks.dk
- nemadgang.dk
- sundhed.dk

Hvorfor understøtter vi stadig SSLv3

Med 15 år på bagen burde vi have lagt SSLv3 i graven og udelukkende benytte nye og sikrere protokoller som TLS1.2. Så hvorfor har vi så ikke gjort det? Tilbage til overskriften på mit blogindlæg, så bunder det i understøttelse af gamle browsere, som ikke længere kan opgraderes. De kan enten ikke opgraderes på grund af det bagvedliggende operativsystem ikke understøtter nyere og sikrere protokoller eller fordi man ikke kan installere nye browserversioner på et gammelt operativsystem. I offentlige udbud har det været meget almindeligt at der stilles krav til understøttelse af Windows XP og IE6. Når det er gået vildt for sig er det kravene skruet op til IE8 på en Windows XP med service pack 3. Argumenterne har næsten altid været, at der internt i myndigheden stadig blev benyttet IE6 på Windows XP arbejdsstationer.

Googlebot Jun 2014	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
IE 6 / XP No FS 1 No SNI 2	Protocol or cipher suite mismatch		Fail 3
IE 7 / Vista	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS	256
IE 8 / XP No FS 1 No SNI 2	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) No FS	112

Hvis man deaktiverer SSLv3 på serveren vil der ikke længere kunne etableres en sikker SSL forbindelse med IE6. Det er prisen med mindre man vil supportere TLS_FALLBACK_SCSV (https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00) , som forhindrer downgrade dance til SSLv3.

Fremtiden?

Vi ser heldigvis ikke længere krav om understøttelse af IE6 i offentlige udbud, men vi skal ikke meget mere end 1 år tilbage før det var meget normalt. Vi ser stadig krav om understøttelse af Windows XP og IE8 - jeg er godt klar over at der stadig er mange brugere derude på disse platforme, men der sker på bekostning af vores alle sammens sikkerhed. Vi er nødt til at understøtte gamle protokoller (som SSLv3 og SHA-1 certifikater (http://www.version2.dk/blog/saa-skal-bestilles-ssl-certifikater-68710)) og vi er nødt at implementere en hel

masse ekstra kode for at tingene fungerer i både moderne browsere og i gamle IE6(7,8). Mere kode betyder større risiko for fejl (herunder sikkerhedshuller), så det ville være dejligt hvis vi endegyldigt kunne lægge Windows XP, IE6(7,8) i graven og sammen bevæge os et trin op af stigen.

Opdateret 20141015-1421: www.sundhed.dk (http://www.sundhed.dk) er faktisk også sårbar da den understøtter SSLv3 med block cipher.

Kilder:

- http://poodlebleed.com/ (http://poodlebleed.com/)
- http://googleonlinesecurity.blogspot.dk/2014/10/this-poodle-bites-exploi... (http://googleonlinesecurity.blogspot.dk/2014/10/this-poodle-bites-exploiting-ssl-30.html)
- http://askubuntu.com/questions/537196/how-do-i-patch-workaround-sslv3-po... (http://askubuntu.com/questions/537196/how-do-i-patch-workaround-sslv3-poodle-vulnerability-cve-2014-3566)
- https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html (https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html)

Om Kim Bjørn Tiedemann

Kim er udviklingschef hos Schultz og arbejder også som løsningsarkitekt og scrum coach. Han har arbejdet med agil udvikling de seneste 5 år, teknologi er hans store passion, og i sin fritid koder han på en Windows 8-app. Han er uddannet i datalogi fra AAU.

Følg @kimtiede 96 følgere