OUCH! | Special Edition

Maandelijkse Security Awareness nieuwsbrief voor Computergebruikers.

OUCH!

IN DEZE EDITIE...

- **Wat is Heartbleed?**
- **Wat te doen?**
- **Pas op met Phishing Pogingen**

Heartbleed – Waarom zorgen maken?

Overzicht

Op maandag 7 april werd een belangrijke kwetsbaarheid ontdekt in één van de de populairste implementaties van het SSL-protocol, nl. OpenSSL. SSL is een zeer belangrijk security protocol op het Internet. Niet enkel voorziet SSL in de encryptie van online communicatie, maar het biedt ook zekerheid dat je verbinding maakt met legitieme websites tijdens het online winkelen of elektronisch bankieren. In deze nieuwsbrief geven we een overzicht van de impact van deze kwetsbaarheid voor jezelf en wat je kan doen om je ertegen te beschermen.

Gastredacteur

Jake Williams (**@MalwareJake**; **malwarejake.blogspot.com**) werkt als Chief Scientist bij CSRgroup Computer Security Consultants. Hij is tevens medeauteur van de SANS cursussen Memory Forensics (FOR526) en Malware Reserve Engineering (FOR610).

Wat Is Heartbleed?

De Heartbleed kwetsbaarheid laat hackers toe om te verbinden met een webserver om gevoelige informatie te verzamelen, zoals jouw gebruikersnaam en wachtwoord. Indien een hacker zulke informatie kan verzamelen, kan deze informatie gebruikt worden om aan te melden op iedere gebruikersaccount dat dezelfde gebruikersnaam en wachtwoord heeft. Ook al bestaat de kwetsbaarheid sinds de laatste twee jaar, het is recent ontdekt en publiek gemaakt op 7 April. Heartbleed heeft geen impact op Windows of Mac computers, maar heeft hoofdzakelijk gevolgen op bekende websites op het Internet, zoals Facebook en Gmail. Om de zaken nog complexer te maken, is niet iedere website geïmpacteerd, maar wel een groot aantal. Om te bepalen of een website kwetsbaar is of niet, biedt Lastpass een handig tooltje aan op https://lastpass.com/heartbleed/.

Wat moet ik doen?

Je kan verscheidene maatregelen treffen om je te beschermen. Deze maatregelen helpen niet enkel voor Heartbleed, maar bieden ook bescherming tegen verschillende andere aanvallen die zich in de toekomst kunnen voordoen:

- Wijzig eerst je wachtwoorden op websites waarvan geweten is dat ze kwetsbaar zijn en die de kwetsbaarheid hebben gepatched. Begin eerst met jouw belangrijkste gebruikersaccounts. Weet je niet of een website kwetsbaar is, wijzig dan sowieso jouw wachtwoord. Maak van deze gelegenheid gebruik om jouw wachtwoorden te wijzigen en jouw online beveiliging te verbeteren.
- Telkens wanneer je jouw wachtwoorden wijzigt, zorg ervoor dat de wachtwoorden moeilijk te raden zijn. Indien de website twee-staps-verificatie ondersteunt, schakel deze dan in. Dit is een handige maatregel om jouw gebruikersaccount beter te beveiligen.
- Zorg ervoor dat je een uniek wachtwoord hebt voor iedere online gebruikersaccount dat je hebt. Indien dan één

Heartbleed – Waarom zorgen maken?

website wordt aangetast, zullen de rest van jouw gebruikersaccounts veilig blijven. Heb je moeite om jouw wachtwoorden te onthouden? Proficiat, dit betekent dat je sterke wachtwoorden gebruikt. We raden aan dat je een wachtwoord manager gebruikt die de wachtwoorden veilig bewaart. Het is een handig hulpmiddel om niet enkel jouw online activiteiten te vergemakkelijken maar ook om ze beter te beveiligen.

- Denk aan jouw email toepassingen! Indien de email toepassing, zoals Outlook of Apple Mail gebruik maakt van SSL om te verbinden met de mail server, dan moet je de wachtwoorden wijzigen.

Indien je meer wenst te weten over deze maatregelen, raadpleeg dan zeker de sectie 'Meer Informatie' aan het einde van de nieuwsbrief.

Om jezelf te beschermen kan je best wachtwoorden van belangrijke gebruikersaccounts aanpassen met een uniek en sterk wachtwoord, dit voor iedere account.

Pas op met Phishing pogingen

Jammer genoeg zijn de slechterikken doorwinterde opportunisten. Ze zien dat Heartbleed een actueel nieuwsitem is en dat veel mensen, waaronder jezelf, erover lezen. Hier zullen ze op inspelen door valse emails op te stellen, waarbij men de indruk geeft dat ze van legitieme partijen komen (zoals banken of winkels). Of doen ze zich voor als beveiligingsbedrijven die gratis tools aanbieden waarbij je kan controleren op de Heartbleed kwetsbaarheid.

Deze tactiek (ook wel bekend als phishing) is niet nieuw. Aanvallers proberen je te overtuigen om op links te klikken die je laten omleiden naar schadelijke websites of overtuigen je om besmette bijlages te openen. Indien je het slachtoffer wordt van dergelijke praktijken, kan je computer mogelijk besmet geraken. Indien je jouw wachtwoord wil veranderen, geef dan het adres van website (ook wel URL genoemd) zelf in via de adresbalk en verander dan online jouw wachtwoord. Op deze manier, ben je zeker dat je de echte en officiële website gebruikt.

Meer informatie

Welke websites zijn kwetsbaar:	https://lastpass.com/heartbleed/
OUCH! Wachtwoorden:	http://www.securingthehuman.org/ouch/2013#may2013
OUCH! Wachtwoord managers:	http://www.securingthehuman.org/ouch/2013#october2013
OUCH! Twee-staps-verificatie:	http://www.securingthehuman.org/ouch/2013#august2013
OUCH! Phishing:	http://www.securingthehuman.org/ouch/2013#february2013
Technische informatie:	https://www.sans.org/webcasts/openssl-heartbleed-vulnerability-98105

Redactie: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Vertaald door: Jan-Adam Breukel