OUCH! | Extraupplaga

Det Månatliga Nyhetsbrevet Om Säkerhetsmedvetenhet för Datoranvändare

OUCH!

I DENNA UTGÅVA…

- Vad är Heartbleed?
- Vad ska jag göra?
- Se upp för nätfiske-attacker

Heartbleed - Varför bryr jag mig?

Översikt

På Måndagen den 7:e April var en allvarlig sårbarhet identifierat i ett av de mest populära implementeringarna av SSL-protokollet, som kallas för OpenSSL. SSL är ett mycket viktig krypteringssystem som används på nätet. Inte bara krypterar SSL din kommunikation på nätet, men det bidrar till att du ansluter till legitima webbplatser när du näthandlar eller gör ett bankärende på nätet. I detta nyhetsbrev ger vi en mycket enkel översikt över vad denna sårbarhet betyder för dig och vad du kan göra för att skydda dig.

Gästredaktör

Jake Williams (**@MalwareJake**; **malwarejake.blogspot.com**) är Vetenskapschef vid CSRgroup Computer Security Consultants. Han är också medförfattare till Memory Forensics (FOR526) och Malware Reverse Engineering (FOR610) kurserna på SANS.

Vad är Heartbleed?

Heartbleed sårbarheten tillåter hackare att ansluta till en webbserver och inhämta känslig information som kan inkludera ditt användarnamn och lösenord. Om en angripare kunde inhämta sådan information, kan de använda den informationen för att logga in på någon av dina konton med samma användarnamn och lösenord. Även om sårbarheten har funnits i de senaste två åren, var det bara upptäckt och offentliggjord den 7:e April. Heartbleed påverkar inte Windows-eller Mac-datorer; det drabbar främst webbplatser på Internet som du använder, till exempel Facebook och Gmail. För att göra saken mer förvirrande, påverkar det inte alla webbplatser på Internet, men det påverkar många av dem. Du kan kontrollera om en webbplats som du använder är eller var utsatt genom att använda Lastpass webbplatsens kontrollverktyg på https://lastpass.com/heartbleed/.

Vad Bör Jag Göra?

Det finns flera åtgärder du kan vidta för att skydda dig. Inte bara kommer dessa åtgärder att skydda dig mot Heartbleed sårbarheten, men de kommer att hjälpa dig skydda dig mot många andra attacker i framtiden:

- Först, ändra ditt lösenord på webbplatser som du vet var sårbara och har lappat sårbarheten, och börja med dina viktigaste konton först. Om du inte vet om en webbplats var sårbar, byt lösenord ändå. Detta är en bra tid för att uppdatera dina lösenord och förbättra din säkerhet på nätet.
- Se till när du uppdaterar dina lösenord att du använder starka, svåra att gissa lösenord. Dessutom, om webbplatsen har stöd för något som kallas tvåstegsverifiering, aktivera det. Detta är ytterligare ett steg som bidrar till att göra din onlinekonton säkrare.
- Se till att du använder ett separat, unikt lösenord för alla dina onlinekonton. På så sätt, även om en webbplats drabbats,

Heartbleed - Varför bryr jag mig?

kommer alla dina andra konton fortfarande att vara säkra. Kommer du inte ihåg alla dina lösenord? Grattis, betyder att du använder starka lösenord. Vi rekommenderar starkt att du använder denna möjlighet att börja använda en lösenordshanterare som lagrar alla dina lösenord säkert. Dessa är bra verktyg som inte bara kan förenkla dina aktiviteter på nätet, men också bidra till att göra dem betydligt säkrare.

- Glöm inte dina e-postklienter. Om din e-postklient, till exempel Outlook eller Apple Mail, använder SSL för att ansluta till e-postservern, kan du behöva ändra dessa lösenord också.

Om du vill ha mer information om några av dessa steg, kolla in avsnittet Resurser i slutet av detta nyhetsbrev.

Det bästa steget för att skydda dig själv är att ändra lösenord på nyckelkonton och se till att använda ett unikt, starkt lösenord för var och en.

Se Upp För Nätfiske

Tyvärr, skurkarna är opportunister. De vet att Heartbleed har varit i nyheterna och en hel del människor, inklusive dig, har läst om det. Som sådana kommer de att skapa falska e-postmeddelanden som ser ut att komma från legitima webbplatser som du använder (till exempel banker eller butiker på nätet). De kan till och med låtsas vara säkerhetsföretag som erbjuder gratis verktyg för att kontrollera för Heartbleed.

Denna taktik (vanligen kallat nätfiske) är inte ny. Angripare försöker lura dig att klicka på länkar som går till skadliga webbplatser eller lura dig att öppna en angripen bilaga. Om du faller offer för dessa attacker kan datorn vara infekterad. Istället, om du behöver ändra ett lösenord, skriver du bara webbplatsens namn (ofta kallad en URL) i webbläsaren och ändra ditt lösenord på nätet. På så sätt vet du att du ansluter till legitim webbplats.

Resurser

OUCH! Lösenord:	https://lastpass.com/heartbleed/
OUCH! Lösenord:	http://www.securingthehuman.org/ouch/2013#may2013
OUCH! Lösenordshanterare:	http://www.securingthehuman.org/ouch/2013#october2013
OUCH! Tvåstegsverifiering:	http://www.securingthehuman.org/ouch/2013#august2013
OUCH! Nätfiske:	http://www.securingthehuman.org/ouch/2013#february2013
Tekniska Detaljer:	https://www.sans.org/webcasts/openssl-heartbleed-vulnerability-98105

Redaktion: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Översatt Av: Andreas Bohman och Marcus Andersson