OUCH! | Spesialutgave

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

- Hva er Heartbleed?
- Hva burde jeg gjøre?
- Vær bevisst på phishing angrep

# Heartbleed – Hvorfor bryr jeg meg?

## Oversikt

Mandag 7. april ble en seriøs svakhet avslørt. Svakheten fantes i en av de mest populære implementasjonene av SSL, kalt OpenSSL. SSL er en veldig viktig sikkerhetsprotokoll som blir brukt gjennom hele Internettet. SSL krypterer ikke bare kommunikasjonen din på nett, den sørger også for at du kobles til riktig nettside når du gjør ting som handel eller nettbank på nett. I dette nyhetsbrevet gir vi deg en enkel oversikt over hva svakheten betyr for deg og hva du kan gjøre for å beskytte deg selv.

**Gjesteredaktør**

Jake Williams (**@MalwareJake**; **malwarejake.blogspot.com**) er forskningssjef hos CSRgroup Computer Security Consultants. Han er også medforfatter av SANS-kursene Memory Forensics (FOR526) og Malware Reverse Engineering (FOR610).

## Hva er Heartbleed?

Svakheten gir angripere mulighet til å koble til en tjeneste på nett og samle inn sensitiv informasjon. Dette kan inneholde ditt brukernavn og passord. Hvis angripere greier å få tak i slik informasjon, så kan de bruke dette til å logge inn på dine kontoer. Svakheten har eksistert i over to år, men den ble ikke offentlig publisert før 7. april i år. Windows og Mac er ikke infisert av svakheten; det er primært en svakhet for tjenere på Internettet, typisk nettsider som Facebook og Gmail. Det som gjør saken enda litt mer forvirrende, er at ikke alle nettsider er påvirket, men mange har vært sårbare. Du kan sjekke om en nettside du bruker er eller har vært sårbar her: https://lastpass.com/heartbleed/.

## Hva burde jeg gjøre?

Det er flere steg du kan ta for å beskytte deg selv. Stegene under vil både beskytte deg mot denne svakheten og mot mange andre angrep i fremtiden:

- Bytt passord på sider du vet var sårbare og som nå har blitt fikset. Start med de viktigste kontoene først. Hvis du er usikker på om et nettsted var sårbar, så bør du bytte passord for å være på den sikre siden. Her kan du benytte muligheten til å oppdatere dine passord og forbedre sikkerheten din.
- Når du oppdaterer passordene, sørg for at du bruker sterke passord som er vanskelig å gjette. Hvis nettsiden støtter to-faktor autentisering, bør du ta i bruk dette. Dette er et ekstra steg som gjør kontoen din tryggere.
- Bruk et unikt passord for hver konto. Hvis du gjør dette så er alle de andre kontoene dine trygge, hvis én skulle bli

# Heartbleed – Hvorfor bryr jeg meg?

kompromittert. Hvis du har fulgt tipset over med å lage sterke passord, så er det nok vanskelig å huske alle passordene. En passordhåndterer kan hjelpe deg med å sikkert lagre passordene. En passordhåndterer kan gjøre det både enklere og tryggere å bruke nettet.

- Ikke glem epostkontoer. Hvis du bruker en epostklient som Outlook eller Apple Mail, bruker denne klienten sannsynligvis SSL for å koble til epost serveren, da må du kanskje bytte disse passordene også.

Hvis du vil ha mer informasjon om noen av disse stegene, sjekk ut ressursene under.

*Det beste steget du kan ta for å beskytte deg er å bytte passord på nøkkelkontoer, samt at du har et sterkt, unikt passord på hver konto.*

## Vær bevisst på phishing angrep

Nettkriminelle er opportunister; de vet at Heartbleed-svakheten har vært mye i nyhetene i det siste og at personer, inkludert deg, har lest om den. For angripere er dette en god mulighet til å lage falske eposter som tilsynelatende kommer fra legitime nettsider (som banker eller nettbutikker). De kan også utgi seg for å være sikkerhetsfirmaer som tilbyr gratis verktøy for å sjekke deg for Heartbleed-svakheten.

Denne teknikken (vanligvis kalt phishing) er ikke ny. Angripere prøver hele tiden å lure deg til å klikke på en link som går til en ondsinnet side eller lure deg til å åpne et infisert vedlegg. Hvis du blir lurt av et slikt angrep, så kan datamaskinen din bli infisert. Hvis du må bytte passordet, tast rett og slett adressen (ofte kalt URL) inn direkte i nettleseren og bytt passord. Hvis du gjør dette kan være sikker på at du kommer til riktig nettsted.

## Ressurser

| | |
|---|---|
| Hvilke sider er sårbare: | https://lastpass.com/heartbleed/ |
| OUCH! Passord: | http://www.securingthehuman.org/ouch/2013#may2013 |
| OUCH! Passordhåndterere: | http://www.securingthehuman.org/ouch/2013#october2013 |
| OUCH! To-steg verifisering: | http://www.securingthehuman.org/ouch/2013#august2013 |
| OUCH! Phishing: | http://www.securingthehuman.org/ouch/2013#february2013 |
| Hva innebærer Heartbleed for brukerne?: | https://norsis.no/2014/04/hva-innebaerer-heartbleed-brukerne/ |
| Tekniske detaljer: | https://www.sans.org/webcasts/openssl-heartbleed-vulnerability-98105 |



Redaksjon: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis