Skrivet av Erik Liljencrantz
2014-04-11 07:08 - Senast uppdaterad 2014-04-11 07:26

Buggen "Heartbleed" som drabbat själva kärnan i säkra överföringar, SSL-protokollet, har uppmärksammats i media. Vi har kollat igenom våra installationer och läget är ***gott***. Buggen har smugit sig in i OpenSSL av senare versioner (version 1.0.1) och kan göra att utomstående kan snappa upp lösenord och kontonummer som skulle överföras krypterade och därmed skyddade från obehöriga.

Här en artikel om "allt man behöver veta":
www.idg.se/2.1085/1.555928/heartbleed---det-har-behover-du-veta
men även SvD och andra "vanliga" tidningar har skrivit:
www.svd.se/naringsliv/nyheter/heartbleed-varre-an-vantat_3452612.svd

Vi har gått igenom våra system och deras användning av SSL, de webbplatser som har https: och kan konstatera att vi inte drabbats:

- huvudwebservern kör en tidigare version av OpenSSL som inte påverkas av Heartbleed
- nya webservern som kommer driftsättas snart hade version 1.0.1 men en snabb uppdatering med "yum update openssl" och omstart av Apache fixade det
- Microsoft IIS skall inte vara drabbad av "Heartbleed"

Så läget är ***gott*** hos oss. Behöver Du hjälp att kolla någon server - hör av Dig :-)