1. Session id tunnistetaan ja järjestelmä ei pyydä, eikä tarkista kirjautumista uudelleen. Sessiota ei ole toteutettu oikein.
2. Sähköpostipalvelu ei lopettanut sessiota, eikä kirjautunut ulos.
3. Kyseessä on XSS-hyökkäys. Jostain tarkistamattomasta syötteestä oltiin pystytty sisällyttämään koodia. Tämä avulla pystyttiin lataamaan haittaohjelmia kirjoittamalla sivun sisältöä uusiksi. Jokin lomake oli huonosti toteutettu, ilman tarkistusta mitä siihen syötetään.
4. XCodeGhost on haittaohjelma, joka vuonna 2015 vaikutti sovelluksiin Applen App Storessa. XCodeGhost on muokattu versio Applen ohjelmistokehitystyökalusta, XCodesta, jota käyttäessä sovelluskehittäjien apeista tuli haitallisia. Niihin sijoitettiin backdoor sekä muita haitallisia ohjelmia kehittäjien tietämättä. Nämä haitalliset sovellukset pääsivät läpi App Storen tarkastusrutiinin, koska verrattuna muihin haittaohjelmiin, siinä ei vaikuttanut olleen mitään erityisesti merkittävää tai haitallista.
5. Heartbleed toimii kysymällä palvelimelta enemmän tietoa, kuin mitä pitäisi saada. Tämä kirjasto sisälsi virhekoodia, joka mahdollisti sensitiivisen tiedon etsimisen palvelimelta. Heartbleediä hyödynnetään lähettämällä väärin muotoiltu sydämenlyöntipyyntö pienellä hyötykuormalla ja suurella kentällä palvelimelle saadakseen vastauksen, jolloin palvelin lähettää tämän kentän pituisen hyötykuorman takaisin. Hyökkääjät voivat lukea jopa 64 kilotavua muistista.