

Apachelta vohkittiin salasanat

14.4.2010 13:21 — Tuomas Linnake
tuomas.linnake@digitoday.fi

Avoimen lähdekoodin Apache Software Foundation joutui "suoran ja kohdennetun" hyökkäyksen kohteeksi verkossa.

Apache-säätiö varoittaa käyttäjiään salasanamurrosta. Hyökkäys alkoi 5. huhtikuuta ja kohdistui säätiön käyttämään palvelimeen. Sillä ajettiin Jira-nimistä seurantaohjelmistoa, jolla pidetään kirjaa Apachen eri ohjelmistohankkeiden ongelmista ja kehitystoiveista.

Ohjelmisto sijaitsi brutus.apache.org-palvelimella, joka käytti Ubuntu Linux 8.04 LTS -käyttöjärjestelmää.

- Jos olet Apachen isännöimän Jiran, Bugzillan tai Confluencen käyttäjä, hash-muotoinen kopio salasanastasi on vaarantunut, Apache ilmoittaa.

Salasanat olivat salattuja, mutta Apache suosittaa niiden vaihtamista joka tapauksessa. Lisäksi Apachen Jiraan 6.-9.huhtikuuta kirjautuneiden pitää olettaa, että salasana on varastettu. Hyökkääjät olivat muuttaneet kirjautumissivun kalastamaan salasanoja.

Seikkaperäinen selvitys

Apache on julkaissut avoimuuden hengessä harvinaisen [seikkaperäisen selvityksen](#) tapahtumien kulusta. Aluksi hyökkääjät avasivat Jirassa uuden tekaistun virhekyselyn ja laittoivat oheen lyhennetyn verkkolinkin.

Useat järjestelmänvalvojat klikkasivat linkkiä, joka käynnisti cross site scripting -hyökkäyksen (xss). Sen avulla valvoilta varastettiin istunnon evästeet. Samaan aikaan hyökkääjät yrittivät runnoa sisään Jiran kirjautumissivulla kokeillen satoja tuhansia salasanyhdistelmiä.

Yksi menetelmästä onnistui. Sen seurauksena hyökkääjät saivat valjastettua Jiran kirjautumissivun hallintaansa. He lähettivät sähköpostia Apache Infrastructure -tiimin jäsenille pyytäen salasanojen nollaamista.

Jäsenet luulivat, että kyseessä on järjestelmän viaton bugi. He

kirjautuivat sisään viesteissä annetuilla tilapäisillä salasanoilla ja muuttivat salasanansa sen jälkeen oikeiksi.

Sama salasanakoitui turmioksi

Yksi näistä salasanoista sattui olemaan sama, kuin erään paikallisen käyttäjän tilissä brutus.apache.orgissa. Tällä käyttäjällä oli lisäksi täydet sudo-oikeudet. Sudo on ohjelma komentojen suorittamiseen toisen käyttäjän oikeuksilla.

Rikolliset saivat Apachen Jira-, Confluence- ja Bugzilla-asennukset sisältävän palvelimen täyteen hallintaansa.

Tapahtuman yksi suuri opetus onkin, että kenenkään ei pitäisi koskaan käyttää samaa salasanaa useassa eri palvelussa. Apachen kohdalla vahinkoa rajoitti se, että kertakäyttösalasanat olivat jo yleisessä käytössä. Jatkossa siitä tehdään pakollista kaikille.

<http://www.digitoday.fi/tietoturva/2010/04/14/apachelta-vohkittiin-salasanat/20105263/66>