Käytä eri avainta SAML ja HTTPS-palveluissa

Shibboleth-konsortio on julkaissut tiedotteen HTTP-liikenteen salaukseen kohdistuvien hyökkäysmekanismien vaikutuksista SAML-viestien vaihtoon. On löydetty haavoittuvuuksia, jotka mahdollistavat palvelimen salaisen avaimen urkkimisen tiettyjä heikkoja algoritmeja ja salaustoteutuksia käytettäessä [1]. Haka-operoinnin suositus on, että SAML-viestien salaamisessa ja allekirjoituksessa käytetään eri avainta, kuin palvelujen HTTP-liikenteen suojaamisessa.

Eri avainten käyttäminen estää SAML-avaimen pääsyn vääriin käsiin, jos HTTP-palvelinohjelmiston toteutuksessa on virheitä. Heartbleed-hyökkäysmekanismi työllisti huomattavasti Haka-operointia ja palvelujen ylläpitoa avaimien vaihdossa.

Haka operoinnin näkemys on, että SAML-viestien vaihdossa käytettävä avain on vaihdettava, mikäli on olemassa epäilys sen joutumisesta vääriin käsiin. Epäilykseksi riittää tieto, että heikko toteutus on ollut saatavilla. Ei riitä perusteeksi olla vaihtamatta avainta, jos heikko toteutus on ollut saatavilla, mutta ei ole tietoa, että sitä olisi hyödynnetty. Sama pätee HTTPS-avaimeen.

Seuraa Shibbolethin tiedotteita

Haka-operointi välittää tietoa Haka-tech postituslistalle kriittisistä tietoturvauhkista. Haka-operointi suosittaa seuraamaan myös suoraan Shibboleth-konsortion tiedotuslistaa. Siellä on hyödyllistä tietoa myös muita SAML-tuotteita käyttäville, sillä tämä kyseinen heikkous koskee kaikkia SAML-tuotteita, joissa käytetään samaa avainta, jota käytetään HTTP-liikenteen salaamiseen.

Lisätietoa

Shibboleth-konsortion tiedote: https://marc.info/?l=shibboleth-announce&m=151673698511556&w=2

Shibboleth postilistat: https://www.shibboleth.net/community/lists/

ROBOT: https://robotattack.org/

Heartbleed: http://heartbleed.com

Briefly in english

Please, see critical security advisory from Shibboleth Consortium.

[1] Tiedotetta tarkennettu 24.1.2018. Vaikuttaa, että ei ole osoitettu ROBOT-haavoittuvuuden aiheuttavan riskiä palvelimen salaisen avaimen paljastumisesta. Sen sijaan voi olla mahdollista tallentaa salattua liikennettä ja myöhemmin purkaa salaus ilman salaista avainta. Tämä saattaa vaarantaa muut salatussa kanavassa välitetyt salaisuudet. Tiedotteessa annettu suositus pätee. Palvelun toteuttajan on arvioitava, onko olemassa epäilys salaisen avaimen joutumisesta vääriin käsiin ja jos on, avain on vaihdettava.