

## Suunnitteluvirhe avasi aukon SSH:hon

19.11.2008 07:58 — Kalevi Nikulainen

SSH-protokollasta on löytynyt suunnitteluvirheestä johtuva protokollatason haavoittuvuus. Protokolla määrittelee paketin pituuden 32-bittinä pitkässä kentässä, kertoo Viestintäviraston tietoturveyskeskös CERT.FI.

CERT-FI:n mukaan kenttää käytetään määrittelemään kuinka paljon tietoa pakettia kohden odotetaan, joten kentän sisältämän tiedon salaus pitää purkaa ennenkuin loput paketista on vastaanotettu ja viestin eheyden tarkistuksessa käytettävä MAC-koodi (Message authentication code) voidaan tarkistaa.

Syöttämällä kohteelle lohkolinen salattua tietoa SSH-paketin ensimmäisenä osana, hyökkääjä voi saada SSH-palvelimen kohteelmaan tuloksena saatavaa selkokielistä tekstiä uuden paketin ensimmäisenä osana. Hyökkääjä voi sen jälkeen syöttää SSH-yhteyteen satunnaisia lohkoja salattua tietoa ja päätellä kuinka paljon tietoa tarvitsee lähettää ennenkuin palvelin päättää koko paketin vastaanotetuksi ja lopettaa vastaanottamisen tuottamalla MAC-virheen.

Virheilmoituksen laukaisemiseen tarvittava määrä tietoa paljastaa tällöin 32-bittisen paketin pituus -kentän sisällön. Lohkosalaimissa käytettyjen Cipher block-chaining (CBC) -tilan ominaisuuksien vuoksi tämän 32-bittisen kentän arvo paljastaa myös saman mittaisen osan lähetetystä paketista selkokielisenä. Lohkoja tarvitsee kuitenkin lähettää SSH-yhteyteen palvelimen toteutuksesta riippuen huomattavia määriä ennenkuin MAC-tarkistus käynnistyy.

SSH eli Secure Shell on protokolla jonka avulla käyttäjät voivat muodostaa turvallisen, salatun yhteyden internetin yli. Sen avulla voidaan esimerkiksi suorittaa komentoja etäjärjestelmässä ja siirtää tiedostoja tietokoneelta tai palvelimelta toiselle. Protokollaa tukevia palvelin- ja asiakassovelluksia, eli server ja client -sovelluksia, on saatavilla useimmille käyttöjärjestelmille. SSH on korvannut käytännössä telnetin ja ftp:n jotka lähettävät muun muassa kirjautumistiedot eli tunnuksen ja salasanan selkokielisenä.

Haavoittuvat ohjelmistot ovat muun muassa OpenSSH

---

4.7p1 sekä muut SSH-protokollaa käyttävät ohjelmistot

CERT-FI:n mukaan ongelman voi poistaa käyttämällä haluttua lohkosalainta CBC-tilan sijaan CTR-tilassa. Esimerkiksi OpenSSH-palvelimessa on toteutettu AES-salaus CTR-tilassa. Halutun algoritmin ja tilan käytön voi helpoiten varmistaa rajoittamalla tarjolla olevaa salausalgoritmien valikoimaa salauksen kättelyvaiheessa.

SSH Communication Securityn tuotteiden korjatuissa versioissa voidaan turvallisesti käyttää CBC-moodia, CERT-FI arvioi.

Lisätietoja löytyy CPNI:n haavoittuvuustiedotteesta [CPNI-957037](#).

<http://www.digitoday.fi/tietoturva/2008/11/19/suunnitteluvirhe-avasi-aukon-sshon/200829886/66>