

F-Securen virustorjunnasta löytyi paha haava

10.2.2005 16:06 — Jaakko Kuivalainen

F-Securen kaikista torjuntaohjelmistoista on löytynyt erittäin vakava haavoittuvuus, jonka avulla hyökkääjä voi mahdollisesti suorittaa omia komentojaan kohdejärjestelmässä. Haavoittuvuus liittyy pakattujen arj-tiedostojen käsittelyyn.

Cert-fin mukaan haavoittuvuus on arj-tiedostojen käsittelyssä tapahtuva puskurinylivuoto.

- Haavoittuvuutta voidaan hyväksikäyttää lähettämällä sähköpostin liitetiedostona tietyllä tavalla muokattu arj-tiedosto tai houkuttelemalla käyttäjä lataamaan tällainen tiedosto esimerkiksi www-sivulta, Cert-fi kertoo.

F-Secure Internet Security- ja Anti-Virus -tuotteiden 2004 ja 2005 -versiot sekä F-Secure Personal Express saavat pikakorjauksen yhtiöltä automaattisesti. Muihin tuotteisiin on ladattava korjaus yhtiön [sivuilta](#).

- Kehotamme kaikkia asiakkaitamme, joihin tämä vaikuttaa, asentamaan päivitykset, ennen kuin joku viruskirjoittajapelle yrittää sitä hyödyntää, F-Securen tutkimusjohtaja **Mikko Hyppönen** kommentoi perjantaina aukkoa yhtiön blogissa.

F-Securen haavoittuvuudelle antama luokitus työasemavirustorjunnan osalta on "korkea" ja palvelin- ja gateway-tuotteille "kriittinen".

Symantec paikkasi ohjelmistoistaan vastaavan upx-tiedostojen käsittelyyn liittyvän haavoittuvuuden keskiviikkona. Sekä [Symantecin](#) että [F-Securen](#) virusskannauksen aukot löysi tietoturvayhtiö Internet Security Systemsin X-Force-tutkimusryhmä.

ISS tietää, että tietoturvayhtiöiden tuotteiden haavoittuvuudet voivat olla erittäin kiusallisia. Yhtiön omien RealSecure- ja BlackICE-tuotteiden haavoittuvuutta hyödyntänyt Witty-mato tuhosi tuhansia koneita viime maaliskuussa. Mato lähti liikkeelle vain muutama päivä päivityksen julkaisun jälkeen.

Päivitys 11.2.2004 klo 10.20: Lisätty Mikko Hyppösen

kommentti.

<http://www.digitoday.fi/tietoturva/2005/02/10/f-securen-virustorjunnasta-loytyi-paha-haava/20058012/66>