

# Vistan asennuslevy käy jokamiehen hyökkäystyökalusta

11.6.2007 16:54

Suomalainen it-asiantuntija Kimmo Rousku julkisti tänään lähes itsestään selvän tietoturvaavoittuvuuden, joka liittyy Windows Vistan asennusmediaan. Microsoftin Kimmo Bergiuksen mukaan kyseessä on kuitenkin tarkkaan harkittu ominaisuus.

Rouskun Windows Vistaan liittyvä tietoturvajulkistus on niin päivän selvä, ettei asiaa ole käsitelty tietoturvaongelmana, vaikka Windows Vista on ollut jo julkaistuna nelisen kuukautta.

Aiemmissa NT-sarjan Windowseissa käyttöjärjestelmän asennusmedia on kysynyt järjestelmäkäyttäjän salasanaa Windowsin palautuskonsolia käynnistettäessä rompulta päin. Windows Vistan asennusrompun palautuskonsoli (recovery console) ei sitä kysy.

## **Kaikki oikeudet muutamalla klikkauksella**

Palautuskonsoliin pääsee muutamalla hiiren klikkaukselta, kun tietokone käynnistetään millä tahansa Windows Vistan asennusrompulla. Lisäksi keinoa voidaan hyödyntää miltä tahansa Vistan WinPE-käynnistysmedialta, joita voidaan tehdä Microsoftin jakamalla WAIK-työkalulla.

Vistan palautuskonsolia voidaan hyödyntää myös vanhempien Windows-versioiden kanssa. Konsolin avulla päästään kaikkiin tietokoneen tietoihin käsiksi oikeusasetuksista riippumatta. Sen avulla voidaan myös upottaa haittaohjelmia. Koneen käynnistäminen ja asennusrompun tai usb-tikun kytkeminen koneeseen vaatii fyysistä pääsyä koneen luokse.

## **Usb- ja verkkotuet helpottavat tietojen varastamista**

Palautuskonsolin avulla voidaan käyttää sekä graafisia että komentoriviohjelmistoja. Myös esimerkiksi verkko- ja usb-ajurit ja toiminnot ovat kytketty päälle. Näin tietoja on helppo varastaa esimerkiksi usb-muistitikun avulla. Lisäksi mistään toimista, lukuun ottamatta tietokoneen sammuttamista ja käynnistämistä, lokeihin ei jää yhtään merkintää.

## **"Tarkkaan harkittu ominaisuus"**

---

Huomattuaan ongelman, Rousku otti yhteyttä Suomen Microsoftin Kimmo Bergiukseen, jonka mukaan ongelma ei ole bugi eikä haavoittuvuus vaan tarkkaan harkittu ominaisuus.

Bergius korostaa, että vaikei ominaisuuden toiminnan muutoksesta ole erikseen varoiteltu tietoturvatiedoissa, on siitä kuitenkin kerrottu ja yhtiö on ennen kaikkea kertonut ja valistanut tavoista, kuten efs- ja bitlocker-salausten käytöstä. Näitä ei Vista-rompulla ohiteta.

Bergiuksen mukaan Microsoftilla ollaan todettu, että silloin kun palautuskonsolia tarvitaan, kovalevy tai Windowsin rekisteri saattaa olla jo niin korruptoitunut, ettei salasanakyselyä pystytä tekemään. Näiden yleisten tukitilanteiden vuoksi salasanakysely on kytketty pois päältä. Jos palautuskonsolin asentaa kiintolevylle, se kysyy käyttäjätunnukset.

Windows on ollut aina haavoittuvainen toisille käynnistyslevyille. Esimerkiksi Linux live -rompuilla ja muistitikuilla ollaan voitu ohittaa ongelma jo vuosia sitten. - Nyt kyse on siitä, että Vistan asennusromppu tekee asiasta todella helppoa, ja kuka tahansa voi sen tehdä, sanoo Rousku. Kaupasta saa halvimman Vista-dvd:n sadan euron pintaan.

### **Helpot suojauskeino**

Sekä Bergiuksen että Rouskun mukaan parhaat keinot estää ongelman hyödyntäminen, on asettaa tietokoneille biosista salasana ja estää muilta kuin c-asemalta käynnistäminen. Oletuksena yleensä romppuasema on käynnistysjärjestyksessä ennen kiintolevyä juuri cd-asennusten vuoksi.

Rousku toivookin, että Windowsin jokaisen version mukana toimitettaisiin samat kryptaustyökalut. Nyt bitlocker ja efs-salaustyökalut saa vain Vistan Enterprise ja Ultimate -versioiden mukana. Myös muilla tietoturvalavalmistajilla on tarjolla levynsalaustyökaluja.

Lisää aiheesta Rousku [hyväksikäyttöesimerkissä](#)

**Kirjoittaja: Matias Mäki**  
[matias.maki@sanoma.fi](mailto:matias.maki@sanoma.fi)

<http://www.itviikko.fi/tietoturva/2007/06/11/vistan->

---

[asennuslevy-kay-jokamiehen-  
hyokkaystyokalusta/200714455/7](http://www.itviikko.fi/asennuslevy-kay-jokamiehen-hyokkaystyokalusta/200714455/7)