

Witty-mato tunkeutuu palomuurin aukosta

20.3.2004 16:53 — Jaakko Kuivalainen

Verkkomato Witty aloitti leviämisensä lauantaina aamulla Suomen aikaa, Viestintäviraston Cert-fi-tietoturvaryhmän varoituksessa kerrotaan. Mato käyttää hyväkseen Internet Security Systemsin BlackICE-ohjelmiston haavoittuvuutta, jolle yhtiö julkaisi paikan torstaina.

Madonreikä liittyy BlackICE-palomuuriohjelmiston protocol analysis module -komponentin tapaan käsitellä icq-verkkoliikennettä. Witty-verkkomato leviää automaattisesti ilman käyttäjän toimia, jos järjestelmässä on paikkaamaton BlackICE-ohjelmisto, Cert-fi-tietoturvaryhmä kertoo.

Mato käyttää leviämiseensä udp-paketteja. Saastuneista järjestelmistä mato yrittää lähettää itsensä satunnaisesti valitsemiinsa 20 000 ip-osoitteeseen. Cert-fi:n mukaan kohdeportit vaihtelevat, mutta lähdeportti on aina udp/4000.

Mahdollisia ikävyyksiä

Tartuntavaiheessa mato toimii ainoastaan järjestelmän muistissa eikä kirjoita levyille mitään.

Leviämisen jälkeen Witty avaa kohdejärjestelmässä satunnaisen fyysisen levyaseman suorittaakseen toistaiseksi tuntemattomia toimia, jotka Cert-fi:n mukaan saattavat olla vahingollisia kohdejärjestelmälle, Cert-fi varoittaa. Cert-fi neuvoo kytkemään haavoittuvat järjestelmät pois verkosta, vaihtamaan turvalliseen palomuurin ja asentamaan ISS:n torstaina julkaisema turvallinen [ohjelmaversio](#).

ISS sai tiedon tuotteidensa haavoittuvuuksista 8. maaliskuuta tietoturvyhtiö eEye Securityltä. Samalle pam-komponentin aukolle ovat alttiita myös ISS:n useat Proventia- ja RealSecure-tuotteet.

Päivitys 21.3. klo 13.30ISS on julkaissut listan tuotteistaan, jotka ovat paikkaamattomana altiina madolle. BlackICE? Agent for Server 3.6 ebz, ecd, ece, ecfBlackICE PC Protection 3.6 cbz, ccd, ccfBlackICE Server Protection 3.6 cbz, ccd, ccfRealSecure® Network 7.0, XPU 22.4 and 22.10RealSecure Server Sensor 7.0 XPU 22.4 and 22.10RealSecure Desktop 7.0 ebf, ebj, ebk,

*ebfRealSecure Desktop 3.6 ebz, ecd, ece, ecfRealSecure
Guard 3.6 ebz, ecd, ece, ecfRealSecure Sentry 3.6 ebz,
ecd, ece, ecf*

<http://www.digitoday.fi/tietoturva/2004/03/20/witty-mato-tunkeutuu-palomuurin-aukosta/20048530/66>