

Linuxin ydin huomattiin haavoittuvaksi Suomessa

22.1.2010 10:22

Oulussa päämajaa pitävä Codenomicon löysi avoimen lähdekoodin Linux-käyttöjärjestelmästä haavoittuvuuden. Ytimen aukko mahdollistaa palvelunestohyökkäyksen.

Suomen Cert-fi-tietoturvaviranomainen toimi jälleen haavoittuvuuden julkaisun koordinoijana löytäjien ja valmistajan välillä. Cert-fi [selvitti äskettäin](#) tätä välillä hankalaakin rooliaan ja julkaisi haavoittuvuuksien koordinoinnin periaatteensa.

[Cert-fi kiittää](#) Codenomiconin **Olli Jarvaa** ja **Tuomo Untista** haavoittuvuuden raportoinnista ja ohjelmistovalmistajaa yhteistyöstä haavoittuvuuden korjaamisessa.

Haavoittuvuus on korjattu Linuxin [versionhallintajärjestelmän lisäyksessä](#). Tällä hetkellä korjaus on sisällytetty vain Linux-ytimen snapshot-versioon.

Osaksi lähdekoodia vuonna 2008

Linux-ytimen haavoittuvuus johtuu virheestä haitallisella tavalla laadittujen ipv6 jumbogram -pakettien käsittelyssä. Hyväksikäyttö perustuisi muotoiltujen pakettien lähettämiseen haavoittuvalle järjestelmälle. Onnistumisen edellytyksenä olisi, että järjestelmässä on network namespaces -optio päällä.

Haavoittuva koodi on liitetty osaksi Linux-ytimen lähdekoodia 8.10.2008. Tätä myöhemmin käännettyt ytimet ovat haavoittuvia. Myös Linux-jakelijoiden ytimet, jotka perustuvat tätä myöhempiin ytimen versioihin tai Linux-ytimen versioon 2.6.31 tai sitä myöhempiin versioihin, voivat olla haavoittuvia.

Kirjoittaja: Tuomas Linnake
tuomas.linnake@digitoday.fi

<http://www.itviikko.fi/tietoturva/2010/01/22/linuxin-ydin-huomattiin-haavoittuvaksi-suomessa/20101040/7>
