

Taannoinen OpenSSL-korjaus jätti aukon

3.10.2007 15:44 — Tuomas Linnake
tuomas.linnake@digitoday.fi

OpenSSL-kirjastoista viime vuonna löydetyt haavoittuvuuden korjauksesta on löydetty off-by-one -virhe, joka voi mahdollistaa palvelunestohyökkäyksen ja teoreettisesti myös mielivaltaisen koodin suorittamisen kohdejärjestelmässä.

Cert-Fi:n mukaan korjaavaa ohjelmistoversiota ei ole julkaistu, mutta [lähdekoodimuotoinen korjaus kylläki](#)osa Linux-jakelijoista on jo julkaissut omat korjaukset.

Haavoittuvat ohjelmistot ovat:

OpenSSL Project, OpenSSL, 0.9.7i
OpenSSL Project, OpenSSL, 0.9.8d

Lisätieto <http://nvd.nist.gov/nvd.cfm?cvename=CVE-2007-5135>
<http://lists.debian.org/debian-security-announce/debian-security-announce-2007/msg00150.html>

<http://www.digitoday.fi/tietoturva/2007/10/03/taannoinen-openssl-korjaus-jatti-aukon/200724438/66>