

Cert-Fi varoittaa viljalti

8.11.2007 16:12 — Tuomas Linnake
tuomas.linnake@digitoday.fi

Viestintäviraston Cert-Fi tykittää usealla tietoturvaruokalla, joista osa, kuten QuickTime ja SonicWall, on kylläkin jo uutisoitu ITviikossa muita lähteitä käyttäen. Keskitytään siis uutuuksiin:

Cert-Fi katsoi aiheelliseksi hälyttää muun muassa Perl-ohjelmointikielen ja PCRE-kirjaston haavoittuvuuksista. Perl ja sen kanssa yhteensopivan PCRE-kirjaston regular expression -toteutuksista on löydetty haavoittuvuuksia, jotka voivat mahdollistaa hyökkääjän oman ohjelmakoodin ajamisen kohdejärjestelmässä.

Perl ja PCRE ovat molemmat laajalti käytettyjä ohjelmistoja, joiden haavoittuvuuksilla voi olla laaja vaikutusalue, Cert-Fi painottaa. PCRE-kirjastoa käytetään muun muassa useissa sähköposti- ja www-palvelinsovelluksissa sekä ohjelmointikielissä. Perl-ohjelmointikielillä on niin ikään toteutettu suuri joukko ohjelmistoja.

Ongelmasta pääsee eroon Perl ja kirjaston päivityksellä. Perl osalta ongelma on korjattu myös kehitysversion 5.9.5 koodijakelussa. Monet Linux-jakelut ovat julkaisseet omat päivityksensä haavoittuvuuksiin.

Lisätietoa löytyy muun muassa [CVE-sivustolta](#).

Oracle Database -tietokantapalvelimesta on puolestaan löytynyt [haavoittuvuus](#), joka voi antaa palvelimelle kirjautuneen käyttäjän suorittaa kohdejärjestelmässä omaa ohjelmakoodiaan. Tähän ei ole olemassa korjausta tai rajoitusta. Oracle Database 10gR2:hta ja tätä aiempia versioita koskeva haavoittuvuus paikataan Oraclen tulevissa päivityksissä.

Kolmanneksi Microsoftin DebugView for Windows -järjestelmäanalyysityökalun Dbgv.sys-kirjastosta on paikallistettu [puutteelliseen käyttäjän syötteen tarkistukseen liittyvä haavoittuvuus](#), joka voi mahdollistaa paikallisen käyttäjän käyttöoikeustason noston.

DebugView ei tosin sisälly Windowsin oletusasennukseen, joten aukko ei ole vakava. Lisäksi korjaus on olemassa.

<http://www.digitoday.fi/tietoturva/2007/11/08/cert-fi-varoittaa-viljalti/200728174/66>