

Microsoft paikkasi kuusi haavoittuvuutta laajalta alueelta

14.5.2008 10:41 — Kalevi Nikulainen

Microsoft on tänään julkaissut neljä ohjelmistopäivitystä, jotka korjaavat kuusi Windows-käyttöjärjestelmän ja sen komponenttien sekä MS Office -sovellusten haavoittuvuutta.

Päivityksistä kolme korjaa korkeimmalta vakavuusluokitukseltaan kriittiseksi luokitellun haavoittuvuuden, kertoo Viestintäviraston tietoturveysyksikkö CERT-FI.

Päivitys MS08-026 korjaa Microsoft Wordista ja Microsoft Word Viewerista kaksi muistin käsittelyyn liittyvää haavoittuvuutta. Haavoittuvuudet liittyvät .doc-tiedostojen tyylisivujen käsittelyyn ja .rtf-tiedostojen merkkijonojen käsittelyyn. Ne mahdollistavat hyökkääjän omien komentojen suorittamisen kohdetietojärjestelmässä. Myös Microsoft Office 2004 for Mac ja Microsoft Office 2008 for Mac ovat haavoittuvia.

Päivitys MS08-027 liittyy Microsoft Publisher -ohjelmistoissa havaittuun haavoittuvuuteen. Haavoittuvuus johtuu muistinkäsittelyvirheestä Publisher-formaatissa olevien tiedostojen käsittelyssä. Haavoittuvuutta hyväksikäyttämällä hyökkääjä voi suorittaa omia komentojaan kohdetietojärjestelmässä. Haavoittuvuutta voi hyväksikäyttää houkuttelemalla käyttäjä avaamaan tietyllä tavalla muotoiltu Publisher-tiedosto.

Päivitys MS08-028 korjaa Windows 2000, XP ja Server 2003-järjestelmissä käytetyssä Microsoft Jet 4.0 Database Engine -komponentissa olevan muistin käsittelyyn liittyvän haavoittuvuuden. Haavoittuvuus mahdollistaa hyökkääjän omien komentojen suorittamisen kohdetietojärjestelmässä. Haavoittuvuutta voi hyväksikäyttää houkuttelemalla hyökkäyksen kohde avaamaan tietyllä tavalla muotoiltu MDB-formaatissa oleva tiedosto. Haavoittuvuuteen on esiintynyt hyväksikäyttöä ja se on julkisesti tiedossa.

Päivitys MS08-029 korjaa kaksi haavoittuvuutta muun muassa Microsoft OneCare, Antigen, Windows Defender

ja Microsoft Forefront -ohjelmistoissa käytetystä Microsoft Malware Protection Engine -komponentista. Haavoittuvuus liittyy Microsoft Malware Protection Enginen tapaan käsitellä tiettyjä tiedostotyyppisiä. Haavoittuvuuksia hyväksikäyttämällä kohdetietojärjestelmässä on mahdollista saada suoritettua palvelunestohyökkäys.

<http://www.digitoday.fi/tietoturva/2008/05/14/microsoft-paikkasi-kuusi-haavoittuvuutta-laajalta-alueelta/200813184/66>