

## NetMail kärsii puskurin triplavuodosta

27.12.2006 09:46 — Tuomas Karvonen

Cert-fi tiedottaa Novell NetMail -palvelinohjelmistoista löytyneistä vakavista haavoittuvuuksista, joita hyväksikäyttämällä hyökkääjän voi olla mahdollista suorittaa kohdetietojärjestelmässä omia komentojaan.

Ensimmäinen haavoittuvuus on nmap-protokollan käsittelyssä tapahtuva puskurin ylivuoto. Palvelinohjelmisto ei tarkista stor-komennon syötteen pituutta. Haavoittuvuuden hyväksikäyttäminen vaatii onnistuneen sisäänkirjautumisen palvelimelle. Toinen haavoittuvuus on imap-protokollan käsittelyssä tapahtuva puskurin ylivuoto. Palvelinohjelmisto ei tarkista riittävästi käyttäjän lähettämän syötteen rakennetta. Tämän aukon hyväksikäyttämiseen ei tarvita sisäänkirjautumista. Kolmas haavoittuvuus on niin ikään imap-protokollan käsittelyssä tapahtuva puskurin ylivuoto. Tässä tapauksessa palvelin ei tarkista riittävästi append-komennolle syötettäviä parametreja. Sisäänkirjautuminen palvelimelle on ehto aukon hyödyntämiselle. Ongelma koskee Novell NetMailin versiota 3.5.2. [Korjaus on saatavilla](#).

<http://www.digitoday.fi/tietoturva/2006/12/27/netmail-karsii-puskurin-triplavuodosta/200624272/66>