

ISS löysi pahan haavan Trend Micron tuotteista

25.2.2005 08:07 — Jaakko Kuivalainen

Trend Micro on paikannut tuotteistaan erittäin vakavan haavoittuvuuden. Aukon löysi samainen Internet Security Systemsin haavoittuvuustutkija **Alex Wheeler**, jonka löytämiä reikiä Symantec ja F-Secure tukkivat aiemmin tässä kuussa.

Trend Micron AntiVirus Library -komponentista löytynyt [ylivuotoaukko](#) liittyy arj-pakattujen tiedostojen käsittelyyn. Sama tiedostomuoto liittyi myös F-Securen tuotteiden haavaan, jonka [yhtiö paikkasi](#) 10. helmikuuta alussa.

Haavoittuvuuden vakavuutta lisää se, että Trend Micron tuotteet ovat yleisiä yhdyskäytävien virustorjunnassa. Yhtiöllä on myös lukuisia operaattoriasiakkaita.

Tavallisilla protokollilla

Muokatun arj-tiedoston avulla hyökkääjä voi saada hallintaansa järjestelmän, joka käyttää Trend Micron haavoittuvaa torjuntaa.

ISS:n mukaan hyökkäykseen ei tarvita autentikointia, ja se todennäköisesti onnistuu oletusasetuksilla. Yhtiö myös arvelee, että hyökkäykseen voidaan käyttää tavallisia protokollia, esimerkiksi smtp:tä, http:tä tai ftp:tä.

Moottorin päivitys paikallaan

Haavoittuvuus altistaa ainakin 30 Trend Micron torjuntaohjelmaa, mukaan lukien yhtiön PC-cillin Internet Security -kuluttajatuotteen sekä useita yhdyskäytävien ja sähköpostipalvelimien virustorjuntaohjelmistoja.

Trend Micro on julkaissut kriittiseksi luokittelemansa [varoituksen](#) asiasta. Yhtiö kehottaa asiakkaitaan päivittämään virustarkistusmoottorin [VSAPI 7.510:een tai uudempaan](#).

Haavoittuvuuden löytänyt Wheeler esiintyy yhdessä kollegansa **Neil Mehtan** kanssa Blackhat Europe -hackeritapahtumassa ensi kuun lopulla. Tutkijoiden esityksen aiheena ovat hyökkäykset virustorjuntaa vastaan - "Owning Antivirus".

Haavoittuvia tuotteita

Trend Micro Client / Server / Messaging Suite for SMB for Windows
Trend Micro Client / Server Suite for SMB for Windows
Trend Micro InterScan eManager
Trend Micro InterScan Messaging Security Suite for Linux
Trend Micro InterScan Messaging Security Suite for Solaris
Trend Micro InterScan Messaging Security Suite for Windows
Trend Micro InterScan VirusWall for AIX
Trend Micro InterScan VirusWall for HP-UX
Trend Micro InterScan VirusWall for Linux
Trend Micro InterScan VirusWall for SMB
Trend Micro InterScan VirusWall for Solaris
Trend Micro InterScan VirusWall for Windows
Trend Micro InterScan Web Security Suite for Linux
Trend Micro InterScan Web Security Suite for Solaris
Trend Micro InterScan Web Security Suite for Windows
Trend Micro InterScan WebManager
Trend Micro InterScan WebProtect for ISA
Trend Micro OfficeScan Corp. Edition
Trend Micro PC-cillin Internet Security
Trend Micro PortalProtect for SharePoint
Trend Micro ScanMail eManager
Trend Micro ScanMail for Lotus Domino on AIX
Trend Micro ScanMail for Lotus Domino on AS/400
Trend Micro ScanMail for Lotus Domino on S/390
Trend Micro ScanMail for Lotus Domino on Solaris
Trend Micro ScanMail for Lotus Domino on Windows
Trend Micro ScanMail for Microsoft Exchange
Trend Micro ServerProtect for Linux
Trend Micro ServerProtect for Windows

Lähde: Trend Micro

<http://www.digitoday.fi/tietoturva/2005/02/25/iss-loysi-pahan-haavan-trend-micron-tuotteista/20058592/66>