

Microsoft korjasi kirjavan joukon haavoittuvuuksia

15.2.2006 09:37 — Jaakko Kuivalainen

Microsoft julkaisi tiistaina tietoturvapäivitykset seitsemälle haavoittuvuudelle. Päivityspäivän teemana oli vain harvoin käyttäjiin vaikuttavat haavoittuvuudet.

Microsoft arvioi kaksi haavoittuvuudesta kriittiseksi. Kaikkein vakavimman tyyppisiä aukkoja ei tiistaina paljastunut; yksikään aukoista ei yhtiön antamien tietojen perusteella sovellu matojen tai bottien levittämiseen verkossa. Vain kolme aukoista altistaa ison osan Windows-käyttäjistä.

Microsoftin MS06-05- ja MS06-06-tiedotteet koskevat Windows Media Player -soitinohjelman haavoittuvuuksia. Kuvatiedostojen käsittelyyn liittyvien haavoittuvuuksien sarja sai jatkoa kriittisestä Bitmap-haavoittuvuudesta Media Playerissa. Uhkana on, että hyökkääjä voi suorittaa haittakoodia houkuttelemalla käyttäjä muokatun kuvatiedoston sisältävälle www-sivulle.

Haavoittuvuus WMP:n plug-inissa

Toinen soitinohjelman aukko koskee vain Windows-järjestelmiä, joissa käytetään jotain muuta selainta kuin Microsoftin Internet Exploreria. Hyödyntämällä aukko hyökkääjä voi päästä suorittamaan haittakoodia koneessa niin ikään oikein muokatun www-sivun avulla tai vaihtoehtoisesti html-sähköpostilla. Microsoftin arvion mukaan päivitys on luokiteltu "tärkeäksi".

Microsoftin MS06-04-tiedote oli toinen kriittisen leiman saaneista. Haavoittuvuus liittyy jälleen Windows Metafile-kuvatiedostojen käsittelyyn, mutta Microsoftin mukaan se koskee vain vanhoja selainversioita Windows 2000 -järjestelmissä. Internet Storm Center huomauttaa, että ei-tuetuista Windows-versioista saattaa löytyä muitakin haavoittuvia kokoonpanoja.

Tiedoteessa MS06-007 yhtiö kertoi Windowsin tcp/ip-protokollapinon palvelunestoaukosta. Windowsin Web Client -palvelusta Microsoft tukki perinteisemmän puskurinylivuodon, jonka hyödyntäminen ei kuitenkaan onnistu ilman kirjautumista järjestelmään. WMP:n Bitmap-

aukon ohella nämä olivat tiistain ainoat haavoittuvuudet, jotka altistavat suuren osan Windows-käyttäjistä.

Kaksi harvinaisempaa reikää

MS06-010:n haavoittuvuus koskee ainostaan PowerPoint 2000 -ohjelmaa ja vaarana on IE:n tilapäistiedostojen sisällön paljastuminen, jos käyttäjä avaa hyökkääjän laatiman PowerPoint-tiedoston.

Harvinaisin aukko oli todennäköisesti tiedotteen MS-009:ssä kuvattu koreankielen merkkien syöttämisen mahdollistavan Input Method Editorin haavoittuvuus. Komponentin korealaisversio ei ole oletuksena asennettuna suomen- tai englanninkielisiin Windows-järjestelmiin tai Office-ohjelmiin.

Microsoftin helmikuun päivityspäivä			
Tiedote			
Vaikutus	Luokitus		
Haavoittuvuus		MS06-004	
Remote Code Execution		Kriittinen	
Win2000/WMF			MS06-005
Remote Code Execution		Kriittinen	
WMP/Bitmap			MS06-006
Remote Code Execution		Tärkeä	WMP/ei-IE-selaimet
			MS06-007
Denial of Service		Tärkeä	Win/TCP/IP
			MS06-008
Remote Code Execution		Tärkeä	Win/Web Client
			MS06-009
Elevation of Privilege		Tärkeä	IME (Korean version)
			MS06-010
Information Disclosure		Tärkeä	PowerPoint2000

<http://www.digitoday.fi/tietoturva/2006/02/15/microsoft-korjasi-kirjavan-joukon-haavoittuvuuksia/20064790/66>