

Vulnerabilidad ANI

Ya hay parche oficial de Microsoft para la vulnerabilidad en los archivos .ANI, .ICO o .CUR

La empresa Microsoft tuvo que moverse rápido por el grave problema que afectaba a sus sistemas operativos y sacar su boletín de seguridad antes del tiempo previsto.

El parche publicado soluciona el problema a:

Microsoft Windows Server 2003 R2 Standard Edition (32-bit x86)
Microsoft Windows Server 2003 R2 Enterprise Edition (32-Bit x86)
Microsoft Windows Server 2003 R2 Datacenter Edition (32-Bit x86)
Microsoft Windows Server 2003 R2 Standard x64 Edition
Microsoft Windows Server 2003 R2 Enterprise x64 Edition
Microsoft Windows Server 2003 R2 Datacenter x64 Edition
Microsoft Windows Server 2003, Standard x64 Edition
Microsoft Windows Server 2003, Enterprise x64 Edition
Microsoft Windows Server 2003, Datacenter x64 Edition
Microsoft Windows Server 2003 Service Pack 1 sobre las siguientes plataformas
Microsoft Windows Server 2003, Standard Edition (32-bit x86)
Microsoft Windows Server 2003, Enterprise Edition (32-bit x86)
Microsoft Windows Server 2003, Datacenter Edition (32-bit x86)
Microsoft Windows Server 2003, Web Edition
Microsoft Windows Server 2003, Enterprise Edition for Itanium-based Systems
Microsoft Windows Server 2003, Datacenter Edition for Itanium-Based Systems
Microsoft Windows Small Business Server 2003 Standard Edition
Microsoft Windows Server 2003 Service Pack 2 sobre las siguientes plataformas
Microsoft Windows Server 2003, Standard Edition (32-bit x86)
Microsoft Windows Server 2003, Enterprise Edition (32-bit x86)
Microsoft Windows Server 2003, Datacenter Edition (32-bit x86)
Microsoft Windows Server 2003, Web Edition
Microsoft Windows Server 2003, Enterprise Edition for Itanium-based Systems
Microsoft Windows Server 2003, Datacenter Edition for Itanium-Based Systems
Microsoft Windows Server 2003, Standard x64 Edition
Microsoft Windows Server 2003, Enterprise x64 Edition
Microsoft Windows Server 2003, Datacenter x64 Edition
Microsoft Windows Server 2003 R2 Standard Edition (32-bit x86)
Microsoft Windows Server 2003 R2 Enterprise Edition (32-Bit x86)
Microsoft Windows Server 2003 R2 Datacenter Edition (32-Bit x86)
Microsoft Windows Server 2003 R2 Standard x64 Edition
Microsoft Windows Server 2003 R2 Enterprise x64 Edition
Microsoft Windows Server 2003 R2 Datacenter x64 Edition
Microsoft Windows Server 2003, Standard Edition (32-bit x86)
Microsoft Windows Server 2003, Enterprise Edition (32-bit x86)
Microsoft Windows Server 2003, Datacenter Edition (32-bit x86)
Microsoft Windows Server 2003, Web Edition
Microsoft Windows Small Business Server 2003 Standard Edition

Microsoft Windows Server 2003, Datacenter Edition for Itanium-Based Systems
Microsoft Windows Server 2003, Enterprise Edition for Itanium-based Systems
Microsoft Windows XP Tablet PC Edition 2005
Microsoft Windows XP Media Center Edition 2005
Microsoft Windows XP Professional x64 Edition
Microsoft Windows XP Service Pack 2 sobre las siguientes plataformas
Microsoft Windows XP Professional
Microsoft Windows XP Home Edition
Microsoft Windows XP Professional x64 Edition
Microsoft Windows 2000 Service Pack 4 sobre las siguientes plataformas
Microsoft Windows 2000 Datacenter Server
Microsoft Windows 2000 Advanced Server
Microsoft Windows 2000 Server
Microsoft Windows 2000 Professional Edition
Microsoft Small Business Server 2000 Standard Edition
Windows Vista Ultimate
Windows Vista Enterprise
Windows Vista Business
Windows Vista Home Premium
Windows Vista Home Basic
Windows Vista Starter
Windows Vista Ultimate 64-bit edition
Windows Vista Enterprise 64-bit edition
Windows Vista Home Premium 64-bit edition
Windows Vista Home Basic 64-bit edition

-MS07-017:

Vulnerabilidad en GDI podría permitir ejecución remota de código

Vulnerabilidad en motor de gráficos (925902)

La actualización corrige hasta siete vulnerabilidades relacionadas todas con el motor de proceso gráficos de Microsoft Windows (Graphics Rendering Engine), donde permiten desde la elevación de privilegios a la ejecución de código.

Les recordamos que es importante actualizar nuestras máquinas para estar a salvo de posibles ataques o fallos en nuestros sistemas.

Fecha artículo: 2007-04-04 10:33:11 - url artículo: <http://www.internautas.org/html/4155.html>

Logos y marcas propiedad de sus respectivos autores.

Los comentarios son propiedad y responsabilidad de cada autor.

© 1998-2009 Asociación de Internautas - <http://www.internautas.org>

Inscrita en el Registro Nacional de Asociaciones con el número 164343 - e-mail: asociacion@internautas.org