UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2005−014

Vulnerabilidades en Microsoft Windows, Internet Explorer y Exchange Server

---

Microsoft ha liberado actualizaciones que solucionan vulnerabilidades críticas en Windows, Internet Explorer y Exchange Server. La explotación de estas vulnerabilidades podría permitir a un intruso no autenticado ejecutar código arbitrario de forma remota o causar una negación de servicio en el sistema afectado.

Fecha de Liberación:	11 de Octubre de 2005
Ultima Revisión:	11 de Octubre de 2005
Fuente:	CERT/CC y diversos reportes de Equipos de Respuesta a Incidentes, así como Foros y Listas de Discusión.

Sistemas Afectados

Microsoft Windows todas las versiones	**MSDTC y COM+**	<KB902400
Microsoft Windows todas las versiones	**Microsoft DirectX**	<KB904706
Microsoft Windows todas las versiones	**Windows Shell**	<KB900725
Microsoft Windows todas las versiones	**Internet Explorer**	<KB896688
Microsoft Windows todas las versiones	**Microsoft Collaboration Data Objects**	<KB907245
Microsoft Windows todas las versiones	**Administrador de conexiones de red**	<KB905414
Microsoft Windows todas las versiones	**Plug and Play**	<KB905749
Microsoft Windows todas las versiones	**Servicio de Cliente para NetWare**	<KB899589
Microsoft Windows todas las versiones	**Cliente FTP de Windows**	<KB905495

Riesgo

Alto

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Múltiples vulnerabilidades

I. Descripción

Los Boletines de Seguridad de Microsoft para Octubre de 2005 cubren vulnerabilidades en Windows e Internet Explorer. Información adicional está disponible en las siguientes Notas de las Vulnerabilidad del US−CERT:

- **VU#214572 − Microsoft Plug and Play falla al validar correctamente los datos proporcionados por un usuario.**

  Microsoft Plug and Play contiene una falla en la manera en como maneja el buffer de mensajes que podría resultar en la ejecución remota o local de código arbitrario o una condición de negación de servicio.
  (CAN−2005−2120)

- **VU#883460 − Buffer Overflow en Microsoft Collaboration Data Objects.**

  Un Buffer Overflow en Microsoft Collaboration Data Objects puede permitir a un intruso remoto no autorizado, ejecutar código arbitrario en el sistema vulnerable.
  (CAN−2005−1987)

- **VU#922708 − El shell de Microsoft Windows falla al manejar archivos de acceso directo.**

  El Shell de Microsoft Windows no maneja apropiadamente algunos archivos de acceso directo y puede permitir la ejecución de código arbitrario cuando un archivo especialmente diseñado es abierto.
  (CAN−2005−2122)

- **VU#995220 − Buffer overflow en Microsoft DirectShow.**

  Un buffer overflow en Microsoft DirectShow puede permitir a un intruso remoto no autenticado ejecutar código arbitrario en un sistema vulnerable.
  (CAN−2005−2128)

- **VU#180868 − Microsoft Distributed Transaction Coordinator es vulnerable a buffer overflow mediante un mensaje de red especialmente diseñado.**

Microsoft Distributed Transaction Coordinator (MSDTC) puede ser vulnerable a una falla que permite a un intruso remoto no autenticado, ejecutar código arbitrario.
(CAN−2005−2119)

- **VU#950516 − Microsoft COM+ tiene una falla en la administración de memoria.**

  Microsoft COM+ contiene una vulnerabilidad debido a un falla de administración de memoria que podría permitir a un intruso tomar el control total de un sistema afectado.
  (CAN−2005−1978)

- **VU#959049 − Varios objetos COM causan corrupción de memoria en Microsoft Internet Explorer.**

  Microsoft Internet Explorer inicializa objetos COM que no fueron llamados para ser usados en el navegador Web. Se han identificado varios objetos COM que podrían permitir a un intruso ejecutar código arbitrario o que deje de trabajar Internet Explorer.

- **VU#680526 − Microsoft Internet Explorer permite a objetos COM no ActiveX ser ejemplificados.**

  Microsoft Internet Explorer inicializa objetos COM que no fueron llamados para ser usados en el navegador Web. Esto podría permitir a un intruso ejecutar código arbitrario o que deje de trabajar Internet Explorer.
  (CAN−2005−0163)

II. Impacto

La explotación de estas vulnerabilidades puede permitir a un intruso remoto no autenticado ejecutar código arbitrario con privilegios SYSTEM o con privilegios del usuario. Si el usuario inició sesión con privilegios administrativos, el intruso podría tomar el control total de un sistema afectado. Un intruso podría también causar una negación de servicio.

III. Solución

- **Aplicar actualizaciones.**

  Microsoft ha proporcionado actualizaciones para estas vulnerabilidades en los Boletines de Seguridad y en el sitio Microsoft Update.

- **Soluciones temporales**

  Consulte las siguientes Notas de Vulnerabilidad del US−CERT para soluciones temporales.

IV. Apéndice A. Referencias

- Proyecto Seguridad en Windows, DSC/UNAM−CERT − http://www.seguridad.unam.mx/windows
- Resumen de Boletines de Seguridad de Microsoft para Octubre 2005 − http://www.microsoft.com/technet/security/bulletin/ms05−oct.mspx
- Nota de Vulnerabilidad del US−CERT VU#214572 − http://www.kb.cert.org/vuls/id/214572
- Nota de Vulnerabilidad del US−CERT VU#883460 − http://www.kb.cert.org/vuls/id/883460
- Nota de Vulnerabilidad del US−CERT VU#922708 − http://www.kb.cert.org/vuls/id/922708
- Nota de Vulnerabilidad del US−CERT VU#995220 − http://www.kb.cert.org/vuls/id/995220
- Nota de Vulnerabilidad del US−CERT VU#180868 − http://www.kb.cert.org/vuls/id/180868
- Nota de Vulnerabilidad del US−CERT VU#950516 − http://www.kb.cert.org/vuls/id/950516
- Nota de Vulnerabilidad del US−CERT VU#959049 − http://www.kb.cert.org/vuls/id/959049
- Nota de Vulnerabilidad del US−CERT VU#680526 − http://www.kb.cert.org/vuls/id/680526
- CAN−2005−2120 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CAN−2005−2120
- CAN−2005−1987 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CAN−2005−1987
- CAN−2005−2122 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CAN−2005−2122
- CAN−2005−2128 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CAN−2005−2128
- CAN−2005−2119 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CAN−2005−2119
- CAN−2005−1978 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CAN−2005−1978
- CAN−2005−2127 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CAN−2005−2127
- CAN−2005−0163 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CAN−2005−0163
- Microsoft Update − https://update.microsoft.com/microsoftupdate

---

El Departamento de Seguridad en Cómputo/UNAM−CERT agradece el apoyo en la traducción, elaboración y revisión de éste Documento a:

- Juan Lopez Morales (jlopez at correo dot seguridad dot unam dot mx)
- Jesús Ramón Jiménez Rojas (jrojas at seguridad dot unam dot mx)

UNAM−CERT
Equipo de Respuesta a Incidentes UNAM
Departamento de Seguridad en Cómputo
E−Mail: seguridad@seguridad.unam.mx
http://www.cert.org.mx
http://www.seguridad.unam.mx

ftp://ftp.seguridad.unam.mx
Tel: 56 22 81 69
Fax: 56 22 80 43