

TechCenter de seguridad

Boletín de seguridad de Microsoft MS12-030 - Importante



Vulnerabilidades en Microsoft Office podrían permitir la ejecución remota de código (2663830)

Publicado: martes, 08 de mayo de 2012

Versión: 1.0

Información general

Resumen ejecutivo

Esta actualización de seguridad resuelve una vulnerabilidad de la que se ha informado de forma pública y cinco vulnerabilidades de las que se ha informado de forma privada en Microsoft Office. Las vulnerabilidades podrían permitir la ejecución remota de código si un usuario abre un archivo de Office especialmente diseñado. Un intruso que aprovechara estas vulnerabilidades podría conseguir el mismo nivel de derechos de usuario que el usuario que ha iniciado sesión. Los usuarios cuyas cuentas estén configuradas con menos derechos de usuario en el sistema correrían un riesgo menor que los que cuenten con derechos de usuario administrativos.

Esta actualización de seguridad se considera importante para todas las ediciones compatibles de Microsoft Excel 2003, Microsoft Excel 2007, Microsoft Office 2007, Microsoft Excel 2010, Microsoft Office 2010, Microsoft Office 2008 para Mac y Microsoft Office para Mac 2011; también se considera importante para las versiones compatibles de Microsoft Excel Viewer y Paquete de compatibilidad de Microsoft Office. Para obtener más información, consulte la subsección **Software afectado y no afectado**, en esta sección.

La actualización de seguridad corrige las vulnerabilidades al modificar la forma en que Microsoft Excel valida los datos al analizar los archivos de Excel especialmente diseñados. Para obtener más información acerca de las vulnerabilidades, consulte la subsección Preguntas más frecuentes (P+F) de la entrada de vulnerabilidad específica en la sección siguiente, **Información sobre la vulnerabilidad**.

Recomendación. Los clientes pueden configurar las actualizaciones automáticas para buscar en línea actualizaciones de Microsoft Update mediante el uso del servicio Microsoft Update. Los clientes que tienen habilitadas las actualizaciones automáticas y configuradas para buscar en línea actualizaciones de Microsoft Update normalmente no tienen que realizar ninguna acción porque esta actualización de seguridad se descargará e instalará automáticamente. Los clientes que no han habilitado las actualizaciones automáticas deben buscar las actualizaciones en Microsoft Update e instalar esta actualización manualmente. Para obtener información acerca de opciones de configuración específicas en las actualizaciones automáticas en ediciones compatibles de Windows XP y Windows Server 2003, vea el artículo 294871 de Microsoft Knowledge Base. Para obtener información acerca de las actualizaciones automáticas en las ediciones compatibles de Windows Vista, Windows Server 2008, Windows 7 y Windows Server 2008 R2, vea Introducción a las actualizaciones automáticas de Windows.

Para administradores e instalaciones empresariales, o usuarios finales que deseen instalar esta actualización de seguridad manualmente, Microsoft recomienda que los clientes apliquen la actualización a la primera oportunidad con el software de administración de actualizaciones o busquen las actualizaciones con el servicio Microsoft Update.

Vea también la sección **Herramientas y consejos para la detección e implementación**, más adelante en este boletín.

Problemas conocidos. En el artículo 2663830 de Microsoft Knowledge Base se señalan los problemas detectados que pueden experimentar los clientes al instalar esta actualización de seguridad. Se documentan asimismo las soluciones propuestas.

↑ Principio de sección

Software afectado y no afectado

El software siguiente se ha probado para determinar las versiones o ediciones que están afectadas. Otras versiones o ediciones han llegado al final de su ciclo de vida o no están afectadas. Para determinar el ciclo de vida del soporte técnico de su versión o edición de software, visite Ciclo de vida del soporte técnico de Microsoft.

Software afectado

Microsoft Office

Conjunto de programas de Microsoft Office y otro software	Componente	Repercusión de seguridad máxima	Clasificación de gravedad acumulada	Actualizaciones reemplazadas
---	------------	---------------------------------	-------------------------------------	------------------------------

Conjuntos de programas y componentes de Microsoft Office

Microsoft Office 2003	Microsoft Excel 2003	Ejecución remota de	Importante	KB2596954 en MS11-096 se
-----------------------	----------------------	---------------------	------------	--------------------------

Conjunto de programas de Microsoft Office y otro software	Componente	Repercusión de seguridad máxima	Clasificación de gravedad acumulada	Actualizaciones reemplazadas
Service Pack 3	Service Pack 3 (KB2597086)	código		reemplaza por KB2597086
Microsoft Office 2007 Service Pack 2	Microsoft Excel 2007 Service Pack 2 ^[1] (KB2597161)	Ejecución remota de código	Importante	KB2553073 en MS11-072 se reemplaza por KB2597161
Microsoft Office 2007 Service Pack 2 (KB2597969)	No aplicable	Ejecución remota de código	Importante	Ninguna
Microsoft Office 2007 Service Pack 3	Microsoft Excel 2007 Service Pack 3 ^[1] (KB2597161)	Ejecución remota de código	Importante	Ninguna
Microsoft Office 2007 Service Pack 3 (KB2597969)	No aplicable	Ejecución remota de código	Importante	Ninguna
Microsoft Office 2010 (ediciones de 32 bits)	Microsoft Excel 2010 (ediciones de 32 bits) (KB2597166)	Ejecución remota de código	Importante	KB2553070 en MS11-072 se reemplaza por KB2597166
Microsoft Office 2010 (ediciones de 32 bits) (KB2553371)	No aplicable	Ejecución remota de código	Importante	Ninguna
Microsoft Office 2010 Service Pack 1 (ediciones de 32 bits)	Microsoft Excel 2010 Service Pack 1 (ediciones de 32 bits) (KB2597166)	Ejecución remota de código	Importante	KB2553070 en MS11-072 se reemplaza por KB2597166
Microsoft Office 2010 Service Pack 1 (ediciones de 32 bits) (KB2553371)	No aplicable	Ejecución remota de código	Importante	Ninguna
Microsoft Office 2010 (ediciones de 64 bits)	Microsoft Excel 2010 (ediciones de 64 bits) (KB2597166)	Ejecución remota de código	Importante	KB2553070 en MS11-072 se reemplaza por KB2597166
Microsoft Office 2010 (ediciones de 64 bits) (KB2553371)	No aplicable	Ejecución remota de código	Importante	Ninguna
Microsoft Office 2010 Service Pack 1 (ediciones de 64 bits)	Microsoft Excel 2010 Service Pack 1 (ediciones de 64 bits) (KB2597166)	Ejecución remota de código	Importante	KB2553070 en MS11-072 se reemplaza por KB2597166
Microsoft Office 2010 Service Pack 1 (ediciones de 64 bits) (KB2553371)	No aplicable	Ejecución remota de código	Importante	Ninguna
Microsoft Office para Mac				
Microsoft Office 2008 para Mac (KB2665346)	No aplicable	Ejecución remota de código	Importante	KB2644354 en MS11-094 se reemplaza por KB2665346
Microsoft Office para Mac 2011 (KB2665351)	No aplicable	Ejecución remota de código	Importante	KB2644347 en MS11-089 se reemplaza por KB2665351

Conjunto de programas de Microsoft Office y otro software	Componente	Repercusión de seguridad máxima	Clasificación de gravedad acumulada	Actualizaciones reemplazadas
Otro software de Microsoft Office				
Microsoft Excel Viewer ^[2] (KB2596842)	No aplicable	Ejecución remota de código	Importante	KB2553075 en MS11-072 se reemplaza por KB2596842
Paquete de compatibilidad de Microsoft Office Service Pack 2 (KB2597162)	No aplicable	Ejecución remota de código	Importante	KB2553074 en MS11-072 se reemplaza por KB2597162
Paquete de compatibilidad de Microsoft Office Service Pack 3 (KB2597162)	No aplicable	Ejecución remota de código	Importante	KB2553074 en MS11-072 se reemplaza por KB2597162

^[1]Para Microsoft Excel 2007, además del paquete de actualizaciones de seguridad KB2597161, los clientes también deben instalar la actualización de seguridad para Paquete de compatibilidad de Microsoft Office (KB2597162) con el fin de protegerse de las vulnerabilidades descritas en este boletín.

^[2]Microsoft Excel Viewer se debe actualizar a un nivel de Service Pack compatible (Excel Viewer 2007 Service Pack 2 o Excel Viewer 2007 Service Pack 3) antes de instalar esta actualización. Para obtener información acerca de los visores de Office compatibles, vea el artículo 979860 de Microsoft Knowledge Base.

Software no afectado

Office y otro software

Microsoft SharePoint Server 2010 y Microsoft SharePoint Server 2010 Service Pack 1

Microsoft Office Web Application Companions (WAC)

Convertidor de archivos con formatos XML abiertos para Mac

Microsoft Visio 2010 y Microsoft Visio 2010 Service Pack 1 (ediciones de 32 bits)

Microsoft Visio 2010 y Microsoft Visio 2010 Service Pack 1 (ediciones de 64 bits)

Microsoft Office Word Viewer

Microsoft Visio Viewer 2010 y Microsoft Visio Viewer 2010 Service Pack 1

Microsoft Works 9

↶ Principio de sección

Preguntas más frecuentes (P+F) relacionadas con esta actualización de seguridad

Información sobre la vulnerabilidad

Gravedad e identificadores de vulnerabilidad

Vulnerabilidad de daños en la memoria relacionada con el formato de archivo de Excel (CVE-2012-0141)

Vulnerabilidad de daños en la memoria relacionada con el formato de archivo de Excel en el objeto OBJECTLINK (CVE-2012-0142)

Vulnerabilidad de daños en la memoria mediante el uso de varios bytes modificados (CVE-2012-0143)

Vulnerabilidad de daños en la memoria relacionada con registros SXLI en Excel (CVE-2012-0184)

Vulnerabilidad del desbordamiento del montón del registro MergeCells en Excel (CVE-2012-0185)

Vulnerabilidad de error de coincidencia de tipo en el análisis de registros de series de Excel que podría provocar la ejecución remota de código (CVE-2012-1847)

Información sobre la actualización

Herramientas y consejos para la detección e implementación Implementación de la actualización de seguridad

Información adicional:

Agradecimientos

Microsoft muestra su agradecimiento a todas las personas que han trabajado con nosotros para proteger a los clientes:

- Omair, por informar de la vulnerabilidad de daños en la memoria relacionada con el formato de archivo de Excel (CVE-2012-0141)
- Omair, por informar de la vulnerabilidad de daños en la memoria relacionada con el formato de archivo de Excel en el objeto OBJECTLINK (CVE-2012-0142)
- Omair, en colaboración con VeriSign iDefense Labs, por informar de la vulnerabilidad de daños en la memoria relacionada con registros SXLI en Excel (CVE-2012-0184)
- Sean Larsson y Jun Mao, en colaboración con VeriSign iDefense Labs, por informar de la vulnerabilidad del desbordamiento del montón del registro MergeCells en Excel (CVE-2012-0185)
- Sean Larsson y Jun Mao, en colaboración con VeriSign iDefense Labs, por informar de la vulnerabilidad de error de coincidencia de tipo en el análisis de registros de series de Excel que podría provocar la ejecución remota de código (CVE-2012-1847)
- Un investigador anónimo, en colaboración con Zero Day Initiative de TippingPoint, por informar de la vulnerabilidad de error de coincidencia de tipo en el análisis de registros de series de Excel que podría provocar la ejecución remota de código (CVE-2012-1847)

↗ Principio de sección

Microsoft Active Protections Program (MAPP)

Para mejorar las protecciones de seguridad de los clientes, Microsoft proporciona información acerca de las vulnerabilidades a los principales proveedores de software de seguridad antes de cada publicación mensual de las actualizaciones de seguridad. De este modo, los proveedores de software de seguridad pueden usar esta información para proporcionar protecciones actualizadas a los clientes mediante su software o dispositivos de seguridad, como, por ejemplo, antivirus, sistemas de detección de intrusiones de red o sistemas de prevención de intrusiones de host. Para determinar si hay disponibles protecciones activas en los proveedores de software de seguridad, visite los sitios web de protecciones activas que proporcionan los asociados, enumeradas en Asociados de Microsoft Active Protections Program (MAPP).

↗ Principio de sección

Soporte técnico

Cómo obtener ayuda y soporte técnico para esta actualización de seguridad

Ayuda para instalar actualizaciones: Soporte de Microsoft Update

Soluciones de seguridad para profesionales de TI: Soporte técnico y solución de problemas de seguridad de TechNet

Ayuda para proteger su equipo con Windows de virus y malware: Solución antivirus y centro de seguridad

Soporte local según su país: Soporte internacional

↗ Principio de sección

Renuncia

La información proporcionada en Microsoft Knowledge Base se suministra "tal cual", sin garantías de ningún tipo. Microsoft renuncia al otorgamiento de toda garantía, tanto expresa como implícita, incluidas las garantías de comerciabilidad e idoneidad para un determinado fin. Ni Microsoft Corporation ni sus proveedores se responsabilizarán en ningún caso de daños directos, indirectos, incidentales, consecuenciales, pérdida de beneficios o daños especiales, aun en el supuesto de que se hubiera informado a Microsoft Corporation o a sus proveedores de la posibilidad de dichos daños. Algunos estados de Estados Unidos no permiten la exclusión o limitación de responsabilidad por daños consecuenciales o incidentales, y, por tanto, la limitación anterior puede no ser aplicable en su caso.

↗ Principio de sección

Revisiones

V1.0 (8 de mayo de 2012): Publicación del boletín.

⤴ Principio de sección

⤴ Principio de página

Microsoft

© 2011

Microsoft.

Reservados todos
los derechos.

[Maneje su perfil](#) | [Contactenos](#) | [Newsletter](#)
[Aviso legal](#) | [Marcas registradas](#) | [Privacidad](#)