CONTENIDO PROVISTO POR

Redmond
THE INDEPENDENT VOICE OF THE MICROSOFT IT COMMUNITY

PATROCINADO POR

Quest™

Windows 10: Es un juego de pelota completamente nuevo para el área de TI

El área de TI del mundo sabía que Windows 7 es historia. Con Windows 10, Microsoft está cambiando la manera en que se realizan las actualizaciones para todo, desde la seguridad hasta la conectividad. Tal como se indica en los artículos para este informe especial de Redmond, el martes de parches nunca será el mismo.

- Microsoft sugiere que los profesionales del área de TI deben adaptarse al proceso de actualización de Windows 10 *Página 1*
- Consulta al servicio avanzado de protección contra amenazas basado en la nube de Windows Defender *Página 4*
- El plan de Microsoft para reducir los tamaños de las actualizaciones de Windows 10 en un tercio *Página 7*
- La versión de parches de Microsoft incluye corrección para los problemas de conexión a Internet de Windows 10 *Página 9*

1105 MEDIA

Microsoft sugiere que los profesionales del área de TI deben adaptarse al proceso de actualización de Windows 10

POR KURT MACKIE

Microsoft ha reiterado su mensaje de renovarse o morir para los profesionales del área de TI a cargo de las actualizaciones y los parches de servidores y clientes de Windows.

Su último aviso es poner esto de manifiesto por segunda vez. En el verano pasado, la empresa anunció que su sistema de entrega de actualizaciones de software cambiaría, a partir de octubre, al modelo de servicio para Windows 10 orientado a la mayoría de sus clientes con soporte y sistemas operativos de servidor. Según el modelo de Windows 10, las actualizaciones

llegan mensualmente y son “acumulativas”, lo que significa que contienen todas las actualizaciones “desde la última versión de línea de base” del sistema operativo.

Este cambio de modelo de actualización de Windows 10 se realizó en octubre para los clientes de Windows 7/8.1, así como las versiones de Windows Server 2008 R2 y Windows Server 2012/R2. También se aplicará a Windows Server 2016.

Los dos anuncios de Microsoft señalan el fin de las prácticas tradicionales del área de TI para la administración de actualizaciones de Windows, llamadas “KB” por los profesionales del área de TI para los artículos de “base de conocimientos” que los alertan sobre los parches. Los parches individuales de Microsoft que arruinaron la funcionalidad en un entorno de computación podrían revertirse. Sin embargo, esa capacidad desapareció el pasado octubre.

Los dos anuncios de Microsoft señalan el fin de las prácticas tradicionales del área de TI para la administración de actualizaciones de Windows, llamadas “KB”.

Ningún parche individual

Según el nuevo esquema, si los profesionales del área de TI tuvieran un problema con un parche individual de Windows, entonces tendrían que revertir a la línea de base de sistema operativo del último mes. Al consultar a Microsoft acerca de si los profesionales del área de TI tenían la capacidad para revertir un parche individual (KB) cuando este nuevo enfoque de actualización de “Windows como servicio” tuvo lugar en octubre, Microsoft indicó:

La respuesta es “No”; no es posible controlar qué KB puede aplicarse, por lo que debería realizarse una copia de respaldo de la reversión completa. Sin embargo, la respuesta es más compleja que un simple no.

La complejidad mencionada anteriormente tiene que ver con la fragmentación general de los parches, que ocurre en los entornos de Windows cuando los profesionales del área de TI aplican actualizaciones de manera selectiva, según Microsoft. Si bien los profesionales del área de TI podrían ver un parche individual incorrecto como un problema que Microsoft debería resolver, Microsoft considera que les corresponde a los socios corregir el problema.

“Si existe un problema, el socio deberá abrir un caso y proporcionar una justificación de la empresa para favorecer el debate con Microsoft”, se explicó en el anuncio de Microsoft.

No queda bien claro qué deberían hacer los profesionales del área de TI si un diálogo de este tipo entre Microsoft y los socios no genera una solución para un parche problemático. Parece que solo podrán revertir su parche acumulativo al mes anterior. Dado este enfoque, los profesionales del área

de TI podrían respaldar la aplicación de parches de actualizaciones de las funciones.

Aunque las actualizaciones de seguridad son otra cuestión. Estarán disponibles, ya que se emiten en actualizaciones acumulativas separadas para las empresas que usan Servicios de actualización de Windows Server o sistemas de administración de System Center Configuration Manager. Como alternativa, las actualizaciones acumulativas de seguridad pueden obtenerse a través del Catálogo de actualizaciones de Microsoft. Microsoft ya no planea emitir actualizaciones de seguridad acumulativas a través de su servicio de actualizaciones de Windows.

Cambie su pensamiento

Los profesionales del área de TI que suelen usar métodos tradicionales de administración de parches deberán cambiar su modo de pensar, sugirió Microsoft:

Con Windows 10, se está adoptando un nuevo modelo. Este modelo nuevo, que se conoce como "Windows como servicio", requiere que las empresas reformulen la implementación y la actualización de Windows. Ya no es un proyecto que ocurre cada tantos años, sino un proceso continuo.

Además, el proceso de actualización de Microsoft incluye un ciclo complejo en el que los profesionales del área de TI deberán hacer un seguimiento de los cambios en las sucursales ("sucursal actual" y "sucursal actual de la empresa"). O bien, tienen la opción de seguir la "sucursal de servicios a largo plazo" con las versiones Enterprise o Education de Windows 10, que permite que las empresas tengan los mayores retrasos entre las actualizaciones. No está muy claro si esos ciclos de Windows 10 también se aplican a las versiones anteriores de Windows.

Hasta el momento, las entregas de actualizaciones mensuales más rápidas de Microsoft con Windows 10 no se hicieron sin problemas.

Hasta el momento, las entregas de actualizaciones mensuales más rápidas de Microsoft con Windows 10 no se hicieron sin problemas. Por ejemplo, en mayo, Microsoft aplicó parches a una actualización de los Servicios de actualización de Windows Server (diseñada para descifrar las actualizaciones de Windows 10) que se realizó con errores en abril y, aun así, requirió pasos de configuración manual que los profesionales del área de TI llevaron a cabo correctamente. Probablemente, muchas empresas esperaron evitar la rutina de la aplicación de parches de Windows 10 durante años manteniendo insistentemente Windows 7. Sin embargo, en octubre de 2016, esa perspectiva segura desapareció. Microsoft parece decir a los profesionales del área de TI que sigan con el programa, de manera muy poco sutil. Aunque, si el software se rompiera en las empresas, posiblemente sería una conversación bilateral. R

Kurt Mackie es productor sénior de noticias de 1105 Enterprise Computing Group.

Consulta al servicio avanzado de protección contra amenazas basado en la nube de Windows Defender

El software antivirus tradicional no puede hacer frente a las amenazas dirigidas a las redes empresariales y, cuando Microsoft creó Windows Defender ATP, tuvo ello en cuenta.

POR ED BOTT

El problema con el software antivirus es que es imperfecto. En el juego del gato y el ratón entre los delincuentes cibernéticos y aquellos que tienen a su cargo la defensa de las redes empresariales y equipos individuales, los delincuentes tienen una ventaja insuperable: solo tienen que tener éxito una vez, mientras que los otros tienen que bloquear cada intento.

Esa realidad es la principal razón por la cual no dedico mucho tiempo a los resultados de las pruebas de software antivirus como los de la prueba de AV, una empresa alemana independiente que ha estado publicando comparaciones de programas antivirus desde hace mucho tiempo.

En los últimos seis meses, más o menos, el software antivirus basado en Windows bloqueó alrededor del 98 % de lo que la prueba de AV llama pruebas de "día cero" y casi (pero no tanto) el 100 % de las conocidas muestras "comodín". Eso suena increíble hasta que uno se da cuenta de que esas cifras elevadas en realidad son una hipótesis optimista, si se usan equipos con total aplicación de parches en un entorno controlado. Si su empresa permite un solo equipo que no tiene todos los parches en la red, no hay ninguna perspectiva de éxito. Y, claro, los atacantes más habilidosos y persistentes, a menudo patrocinados por un estado nacional, tienen habilidades y recursos que superan los del atacante promedio.

De modo que no sorprende que muchos expertos en seguridad recomienden que los administradores de empresas adopten una postura más agresiva y asuman que, incluso con la capacitación adecuada y la implementación de la mejor infraestructura de seguridad, algunos atacantes irrumpirán.

De modo que no sorprende que muchos expertos en seguridad recomienden que los administradores de empresas adopten una postura más agresiva y asuman que, incluso con la capacitación adecuada y la implementación de la mejor infraestructura de seguridad, algunos atacantes irrumpirán.

Claro que esto no significa que el software antivirus tradicional sea obsoleto, pero esos programas son solo una pequeña parte de una estrategia de seguridad de múltiples capas. Si desea ver dónde está ocurriendo la innovación real, consulte el servicio avanzado de protección contra amenazas basado en la nube de Windows Defender (Windows Defender ATP), que Microsoft anunció en marzo de 2016 y ahora se está extendiendo a clientes empresariales en todo el mundo después de una extensa vista previa.

Windows Defender ATP es, por excelencia, un producto de Microsoft, empezando por la confusión de marca que parece ser necesaria para cualquier producto nuevo de Windows. Si bien comparte parte de su nombre con Windows Defender, el servicio nuevo tiene poco en común con el software antimalware, que se incluye gratis con Windows 10. En cambio, en un diseño que es típico de casi cualquier producto de Microsoft hoy en día, es un servicio en la nube basado en Azure.

Para la instalación de Windows Defender ATP en un equipo se requieren las versiones Pro, Education o Enterprise, una cuenta de Azure Active Directory y una licencia para el servicio de Windows Defender ATP. El proceso de configuración permite una recopilación de lo que Microsoft

llama “sensores de comportamiento de endpoints”, los cuales realizan un seguimiento de las actividades en cada dispositivo tales como llamadas de registro, actividad de procesos y archivos y comunicaciones de red. Los datos se almacenan en un repositorio privado y aislado en la nube, dedicado a su empresa, y no se comparte con otros suscriptores de Windows Defender ATP. Microsoft publicó detalles sobre Windows Defender ATP en el Centro del área de TI de Windows. Allí también se puede encontrar otro informe sobre las políticas de privacidad y almacenamiento de datos.

El verdadero valor de Windows Defender ATP proviene del análisis que proporciona Microsoft en el que se usa un gráfico de seguridad creado a partir de servicios, como el servicio de reputación de URL de SmartScreen y la Herramienta de eliminación de software malicioso de Microsoft. Además, la información de seguridad de Windows Defender ATP aprovecha la inteligencia de las amenazas de grupos dentro de Microsoft y de socios, como FireEye. En conjunto, los datos específicos masivos posibilitan la identificación del plazo de un ataque, así como las herramientas y las técnicas que los atacantes usaron para eludir las defensas tradicionales anteriores. Incluso, la base de conocimientos incluye información específica sobre “detalles de actores y contexto de intentos” en la que, literalmente, se mencionan los autores de un ataque en función de las técnicas que usaron.

Se presenta en un portal bien organizado que cualquier persona que alguna vez haya administrado una cuenta de Azure debería conocer. Puede recibir alertas de actividades sospechosas, ver las amenazas activas y filtrar la lista para mostrar las amenazas que se corrigieron y aquellas que no.

Puede recibir alertas de actividad sospechosa, ver amenazas activas y filtrar la lista para mostrar las amenazas que se corrigieron y aquellas que no.

Irónicamente, muchas de las empresas que pudieron beneficiarse de Windows Defender ATP podrían ignorarlo por su nombre. Pero, aquellas que entienden que es más que un software antivirus tradicional deberían mirar más de cerca. **R**

Ed Bott es un MVP de Microsoft y un premiado periodista especializado en tecnología que ha brindado cobertura para Microsoft durante 25 años. Escribió diversos libros sobre Windows y Office, incluida la serie de mayor venta de “Inside Out”, de Microsoft Press. Bott ofrece consejos honestos sobre una amplia variedad de temas de tecnología en su blog de ZDNet, “The Ed Bott Report” (El informe de Ed Bott).

El plan de Microsoft para reducir el tamaño de las actualizaciones de Windows 10 en un tercio

POR KURT MACKIE

Una nueva tecnología de Microsoft, conocida como "Plataforma de actualización unificada", promete reducir el tamaño de las actualizaciones futuras de Windows 10 en un tercio.

Como se explicó en Microsoft, esta tecnología emergente podría reducir los tamaños de descarga de Windows 10 "aproximadamente un 35 % cuando se actualiza una importante actualización de Windows a otra". También se prevé que la cantidad del tiempo de procesamiento se reduzca con esta nueva tecnología.

Algunos evaluadores de dispositivos móviles del Programa Windows Insider que usa Windows 10 versión 14959 pronto pudieron ver los efectos de la tecnología de la Plataforma de actualización unificada. Según la promesa de Microsoft, tendrá un beneficio extra para ellos porque permitirá a los usuarios de dispositivos móviles actualizar a la versión más reciente de Windows 10 todo al mismo tiempo, en lugar de hacerlo gradualmente.

Los usuarios de equipos que participan en el Programa Windows Insider también verán versiones de actualizaciones de Windows 10 más pequeñas de la tecnología de Plataforma de actualización unificada.

Los usuarios de equipos que participan en el Programa Windows Insider también verán versiones de actualizaciones de Windows 10 más pequeñas de la tecnología de Plataforma de actualización unificada, según lo sugerido en Microsoft.

Finalmente, Microsoft planea implementar la Plataforma de actualización unificada con otros productos basados en Windows 10, como los dispositivos de Internet de las cosas y los dispositivos de realidad aumentada de Microsoft HoloLens. El plazo para una implementación general y lista para la producción no se indicó en el anuncio de Microsoft.

Microsoft lanza las versiones de Windows 10 mensualmente. También ofrece periódicamente actualizaciones importantes de sistema operativo, que ocurren varias veces al año. Las actualizaciones mensuales son "acumulativas", lo que significa que pueden contener todas las versiones de actualizaciones anteriores. En consecuencia, el tamaño de las actualizaciones de Windows 10 puede ser algo grande, superior a 3 GB,

lo cual puede ser problemático para los dispositivos móviles con espacio de almacenamiento insuficiente.

El problema de tamaño de actualización se aborda en parte a través de la tecnología del "paquete de descarga diferencial", que incluye los bits cambiados, en lugar de una descarga completa, según lo informado en el anuncio de Microsoft. Aparentemente, el enfoque forma parte del próximo esquema de Plataforma de actualización unificada.

Tal vez, la Plataforma de actualización unificada resulte útil para los usuarios finales individuales. En cuanto a la administración del área de TI, Microsoft cuenta con la función de optimización de distribución de Windows Update, que puede refinarse mediante la configuración de la Política de grupos. Es un esquema de actualización de cliente punto a punto que se inició con la "actualización aniversario" de Windows 10 versión 1607, lanzada en agosto. La solución de optimización de distribución está diseñada para descargar los bits de actualización desde los equipos y los bits de actualización desde los centros de datos de Microsoft, como una manera de reducir el posible consumo de ancho de banda que muchas empresas pueden enfrentar durante las actualizaciones de Windows 10. Supuestamente, el esquema reaprovecha la parte no utilizada de la capacidad de carga de una red para realizar las actualizaciones del equipo.

Los usuarios de System Center Configuration Manager disponen de una alternativa a la función de optimización de distribución, que se conoce como "Caché del cliente". Se implementó con la versión preliminar 1604, pero estará disponible en una versión posterior de System Center Configuration Manager, según lo mencionado en el artículo de TechNet. En un análisis inicial de la versión preliminar de la Caché del cliente, como se describe en la publicación del blog de mayo por parte de la consultoría de administración 1E, se determinó que tenía algunos aspectos irregulares en ese momento.

BranchCache es otro sistema de Microsoft más respetado para la administración de problemas de ancho de banda, en especial con las actualizaciones remotas.

BranchCache es otro sistema de Microsoft más respetado para la administración de problemas de ancho de banda, en especial con las actualizaciones remotas. BranchCache está diseñado para empresas con operaciones extendidas y está disponible a través de las versiones Enterprise o Education de Windows 10, aunque algunas de sus capacidades de BITS se incluyen en la versión Pro. BITS, o Servicio inteligente de transferencia de archivos en segundo plano, es una tecnología de Microsoft para administrar el plazo de las transferencias de archivos dentro de una red. R

Kurt Mackie es productor sénior de noticias de 1105 Enterprise Computing Group.

La versión de parches de Microsoft incluye corrección para los problemas de conexión a Internet de Windows 10

POR KURT MACKIE

La publicación reciente de "Martes de parches" de Microsoft contiene una corrección para un problema de conexión a Internet que, supuestamente, tuvo efectos generalizados en los equipos con Windows 10.

La publicación reciente de "Martes de parches" de Microsoft contiene una corrección para un problema de conexión a Internet que, supuestamente, tuvo efectos generalizados en los equipos con Windows 10.

Los problemas de conexión a Internet o Wi-Fi comenzaron recientemente. Microsoft reconoció los problemas en un foro de debate, en el que se indicó lo siguiente: "algunos clientes están teniendo dificultad para conectarse a Internet". En un artículo de soporte, Microsoft aconsejó a los usuarios reiniciar sus equipos, no apagarlos. También se indicó a los usuarios que busquen otros orígenes posibles del problema, como problemas del módem por cable o de conexión del proveedor del servicio de Internet.

Microsoft indicó que el parche KB3206632, que se publicó e incluyó en la publicación reciente del boletín de seguridad, está diseñado para corregir el problema. Este parche reemplaza la actualización KB3201845, que supuestamente era la que provocaba los problemas de conexión a Internet, aunque el autor de InfoWorld, Woody Leonhard, observó que esos problemas ocurrieron dos días antes del lanzamiento de KB3201845.

El problema de conexión a Internet solo afectó a dispositivos con "Windows 10 1607 (RS1)," según lo expresado por Nathan Mercer, evangelizador técnico de Microsoft, en una publicación de lista de servidor de Patchmanagement.org. Pero, hasta el momento, esa es toda la información que Microsoft brindó acerca del problema.

Entonces, posiblemente Microsoft corrigió un problema que nunca describió por completo.

El boletín sobre KB3206632 de Microsoft no es muy descriptivo, aunque sí indica una corrección, realizada en diciembre, para una "falla de servicio en CDPSVC que, en algunos casos, se debió a que los equipos no pudieron adquirir una dirección IP". En una descripción del problema, realizada por The Register, se sugirió que una actualización de software de Microsoft de alguna manera había roto el Protocolo de configuración dinámica de host, utilizado para emitir las direcciones IP.

Entonces, posiblemente Microsoft corrigió un problema que nunca describió por completo. La descripción parece ser una práctica anterior abandonada con el nuevo enfoque ágil de distribución de software de Windows 10.

Microsoft también publicó 12 boletines de seguridad en su parche de diciembre, donde se abordaron seis imperfecciones "críticas". Los elementos principales del "índice de explotabilidad" ese mes incluyen una vulnerabilidad de daño en la memoria del motor script, una vulnerabilidad de daño en la memoria de navegador y una imperfección de omisión de la función de seguridad de Office, entre otras cosas, según lo descrito en el boletín de diciembre. R

Kurt Mackie es productor sénior de noticias de 1105 Enterprise Computing Group.