GE Healthcare

Sitio web de seguridad de Invasive Cardiology

Intervención - Invasive Cardiology

Grupo de productos:	Productos de intervención invasiva
Productos:	Sistemas de registro Mac-Lab IT/XT/XTi, CardioLab IT/XT/XTi, SpecialsLab y ComboLab IT/XT/XTi, y Centricity Cardiology Data Management Systems
Versión:	6.9.6, versión 3
Asunto:	Información de seguridad
Fecha:	9 de marzo de 2018

Resumen

La siguiente información se proporciona a los clientes de GE Healthcare Technologies para informarles de una serie de vulnerabilidades técnicas de seguridad relacionadas con los sistemas de registro Mac-Lab® Hemodynamic, CardioLab® Electrophysiology, SpecialsLab y ComboLab IT para laboratorios de cateterismo, electroforesis y otros laboratorios de intervención, así como con Centricity® Cardiology Data Management Systems.

Configuración básica de los parches de seguridad

La configuración básica de los parches de seguridad de los productos Mac-Lab IT/XT/XTi y CardioLab IT/XT/XTi en el momento de su publicación se recoge en MLCL Base Configuration (Configuración básica de MLCL), en la sección Hemodynamic, Electrophysiology and Cardiovascular Information Technologies (Tecnologías de la información hemodinámicas, electrofisiológicas y cardiovasculares) del sitio web: http://www3.gehealthcare.com/en/Support/Invasive_Cardiology_Product_Security.

Proceso

Las acciones siguientes se realizan siempre que se publica un nuevo parche de seguridad de Microsoft o del fabricante:

- El equipo de ingeniería de Invasive Cardiology realiza un proceso de análisis de seguridad del hardware/software compatible con Mac-Lab IT/XT/XTi, CardioLab IT/XT/XTi, GE Client Review y INW Server.

- Si se encuentra una vulnerabilidad que cumple con los criterios de validación de Mac-Lab IT/XT/XTi y CardioLab IT/XT/XTi, esta se comunica a través de la base de datos de seguridad de los productos de GEHC y del sitio web de seguridad de Invasive Cardiology en las tres semanas posteriores a la publicación del parche.
- Tras la validación de la vulnerabilidad de Mac-Lab IT/XT/XTi y CardioLab IT/XT/XTi, se actualizan la base de datos de seguridad de los productos de GEHC y el sitio web de seguridad de Invasive Cardiology, así como las instrucciones de instalación del parche de seguridad de Mac-Lab IT/XT/XTi y CardioLab IT/XT/XTi afectado.

Los criterios de validación de vulnerabilidad de Mac-Lab IT/XT/XTi y CardioLab IT/XT/XTi son los siguientes: cualquier vulnerabilidad que permita que el malware modifique o deniegue la funcionalidad de Mac-Lab IT/XT/XTi y CardioLab IT/XT/XTi, o que infecte y se propague mediante el uso normal del sistema.

Los clientes son responsables de mantenerse al día con las notificaciones sobre vulnerabilidad de Microsoft y de visitar los sitios web de Invasive Cardiology para comprender las consecuencias de estas en Mac-Lab IT/XT/XTi y CardioLab IT/XT/XTi. Tras la validación de un parche de seguridad, los clientes son responsables de la instalación de los parches de seguridad. Todas las instrucciones de instalación de los parches de seguridad de Mac-Lab IT/XT/XTi y CardioLab IT/XT/XTi están disponibles en la tabla de parches validados del sitio web de seguridad de Invasive Cardiology.

Las vulnerabilidades a las que se expongan los productos Mac-Lab IT/XT/XTi y CardioLab IT/XT/XTi tras su comercialización y que no cumplan los criterios de validación no se recogen en la base de datos de seguridad de los productos de GEHC ni en el sitio web de seguridad de Invasive Cardiology. Se considera que estas vulnerabilidades no son críticas o que están fuera del flujo de trabajo clínico normal de los sistemas Mac-Lab IT/XT/XTi, CardioLab IT/XT/XTi y Centricity INW, por lo que no se validarán. Los parches que no aparezcan en esta tabla no deben instalarse en los productos con el fin de eliminar los riesgos de un funcionamiento incorrecto o de una avería.

CONTENIDO

Historial de las revisiones

Revisión	Fecha	Comentarios
1.0	22 de septiembre de 2017	• 6.9.6 Separación de documentos • KB4025341 validado - Paquete de actualizaciones mensual de julio • Adición de la sección 6.9.6, Rutas de instalación para simplificar la instalación de parches • Parches de septiembre sin validar
2.0	13 de octubre de 2017	• Adición de instrucciones para deshabilitar el protocolo SMB1
3.0	27 de octubre de 2017	• Parches de octubre sin validar
4.0	20 de noviembre de 2017	• Adición de parches de octubre sin validar
5.0	11 de diciembre de 2017	• Parches de noviembre sin validar
6.0	20 de diciembre de 2017	• Para el parche mensual de octubre, se ha añadido una declaración que prescribe la desinstalación de los parches mensuales anteriores antes de instalar el parche mensual de octubre en el servidor
7.0	26 de enero de 2018	• Paquetes de actualizaciones mensuales de noviembre y diciembre validados con otros parches. También se han añadido los parches de enero sin validar.
8.0	9 de marzo de 2018	• Adición del parche de febrero sin validar • Cambio de la longitud mínima definida para la contraseña • Cambio en la redacción de "Actualización del parche" a "Actualizaciones de los parches" • Recomendaciones de seguridad adicionales para los sistemas MLCL

Recomendaciones de seguridad adicionales para los sistemas MLCL

Es aconsejable que siga los consejos que se describen a continuación y las recomendaciones que se incluyen en la Guía de seguridad de MLCL.

- Aplicación de medidas de creación de contraseñas y establecimiento de procesos de gestión de cuentas que refuercen la seguridad
- Sustitución de la contraseña predeterminada por una contraseña más compleja, más segura y única para las cuentas de los usuarios
- Zonas desmilitarizadas y perímetros de defensa para la red del centro
- Uso de firewall de red
- Prevención del acceso a Internet en sistemas MLCL
- Sistemas de detección de intrusiones y de protección contra las mismas

- Redes privadas virtuales (VPN)
- Análisis del tráfico de red
- Seguridad física mejorada
- Análisis de registros
- Aplicación del contenido de la sección Actualizaciones de seguridad opcionales de MLCL v6.9.6

Instalación de los parches de seguridad en los sistemas MLCL

Requisitos:

- Las actualizaciones podrán aplicarse en cualquier momento en que las aplicaciones Mac-Lab IT/XT/XTi, CardioLab IT/XT/XTi o SpecialsLab no estén abiertas.
- Las actualizaciones deben volver a aplicarse si se restablece la imagen inicial del sistema.
- Las actualizaciones se aplican tanto a los sistemas en red como a los sistemas independientes.
- La práctica recomendada consiste en actualizar todos los sistemas MLCL pertinentes del centro.

Este documento se aplica solo a la versión 6.9.6R3. Antes de continuar, compruebe que está utilizando la versión 6.9.6 mediante el procedimiento siguiente:

1. Ejecute la aplicación Mac-Lab CardioLab.
2. Seleccione ***Ayuda > Acerca de Mac-Lab*** (o ***CardioLab***, según corresponda).
3. Compruebe que el número es **6.9.6, versión 3**.
4. Haga clic en ***Cerrar***.
5. Cierre la aplicación.

Recomendación: Utilice Internet Explorer (IE) para descargar el catálogo. Si está utilizando la función de carro para descargar los parches, tendrá que abrirlo en otra ficha o abrir una ventana nueva de http://catalog.update.microsoft.com para verlo.

Cómo iniciar sesión en los sistemas de adquisición y revisión

Cuando se ejecuta un sistema de adquisición o revisión Mac-Lab, CardioLab o SpecialsLab, se aplica una secuencia automática de inicio de sesión, por lo que inicia sesión automáticamente en el sistema operativo. Para instalar un parche de seguridad, el usuario debe haber iniciado sesión como **mlcltechuser**.

NOTA: La información sobre la contraseña se encuentra en el manual de la guía de seguridad. De no ser así, póngase en contacto con el administrador del sistema o con el servicio de asistencia técnica de GE para obtener información sobre la contraseña actual.

1. Encienda el sistema de adquisición.
2. El sistema arranca y muestra la pantalla del ***intérprete de comandos personalizado***.
3. Pulse **Ctrl + Acción + Supr**.
4. Haga clic en ***Cerrar sesión***. En Windows XP, vuelva a hacer clic en ***Cerrar sesión***.
5. Haga clic en ***Aceptar***.
6. Inmediatamente después, mantenga pulsada la tecla **Mayús** hasta que se muestre la ventana de inicio de sesión.
7. Inicie sesión desde su equipo en el sistema operativo como **mlcltechuser**.
8. Inicie sesión desde su equipo en el ***intérprete de comandos personalizado*** como **mlcltechuser**.

Cómo iniciar sesión en Centricity Cardiology INW Server

La información sobre la contraseña se encuentra en el manual de la guía de seguridad. De no ser así, póngase en contacto con el administrador del sistema o con el servicio de asistencia técnica de GE para obtener información sobre la contraseña actual. Inicie sesión en INW Server como **administrador**.

Cómo iniciar sesión en los sistemas de solo software MLCL

Puesto que los sistemas de solo software son compatibles con el cliente, se debe haber iniciado sesión en el sistema con una cuenta de **administrador**.

Cómo instalar el firmware de la impresora

El cliente deberá proporcionar el sistema que instalará el firmware en la impresora.
NOTA: El sistema Mac-Lab/CardioLab no se debe utilizar para descargar o aplicar el firmware de la impresora.

- Utilice el enlace de descarga de la tabla.
- Seleccione la impresora que corresponda.
- Seleccione el idioma inglés y el sistema operativo MLCL pertinente.
- Seleccione el idioma inglés y, en la categoría de firmware, seleccione la utilidad de actualización de firmware correspondiente y haga clic en Descargar.
- Inicie el programa de instalación de firmware y siga las instrucciones para completar la actualización del firmware.

Cómo actualizar el firmware del motor de gestión de Intel (HP Z440): HPSBHF03557 Rev. 1

1. Inicie sesión en el sistema operativo Windows y en el ***intérprete de comandos personalizado*** de MLCL como **mlcltechuser**.
2. Vaya a la sección *Actualizaciones del parche de MLCL V6.9.6* que contiene el archivo de actualización del firmware del motor de gestión de Intel: **sp80050.exe**.
3. Con el botón derecho del ratón, haga clic en el archivo **sp80050.exe** y seleccione ***Ejecutar como administrador***.
4. Haga clic en ***Sí*** en el cuadro de diálogo Control de cuenta de usuario.
5. Haga clic en ***Siguiente*** en el asistente InstallShield.
6. Acepte el contrato y haga clic en ***Siguiente***.
7. Pulse **S** en el indicador de comandos que indica "¿Desea actualizar el firmware del motor de gestión ahora [S/N]?".
8. Reinicie el sistema cuando se haya completado la actualización del firmware.

Pasos para verificar que la actualización del firmware se ha realizado correctamente:

1. Después de reiniciar el sistema, pulse **F10** en la pantalla HP para acceder al menú de configuración.
2. Vaya a ***Principal > Información del sistema***.
3. La versión del firmware del motor de gestión debe ser ***9.1.41.3024***.

Instrucciones de actualización de la BIOS de Z440 a la versión 2.34:

1. Vaya al sitio web HP Customer Support - Software and Driver Downloads (Soporte al cliente de HP - Descargas de software y controladores):

   https://support.hp.com/us-en/drivers/selfservice/hp-z440-workstation/6978828
2. Seleccione ***BIOS***.
3. Seleccione ***Descargar*** la BIOS 2.34 Rev.A del sistema de estaciones de trabajo HP Z440/Z640/Z840.
4. Inicie una sesión en el equipo z440 como ***administrador***.
5. Ejecute el archivo ***sp80745.exe*** descargado.
6. Seleccione ***Sí*** para permitir la ejecución.
7. Seleccione ***Acepto los términos del Contrato de licencia***.
8. Seleccione ***Ver contenido de la carpeta HPBIOSUPDREC***. Se abre la carpeta:

   C:\\swsetup\SP80745\HPBIOSUPDREC
9. Ejecute el archivo ***HPBIOSUPDREC.exe***.

10. Seleccione ***Sí*** para permitir la ejecución.
11. Tras varios segundos, se crea un archivo de registro y aparece una ventana de la herramienta de instalación. Seleccione ***Actualizar*** y ***Siguiente***.
12. Siga las instrucciones de la pantalla y seleccione ***Reiniciar***.
13. La actualización de la BIOS tardará unos minutos; no desconecte la alimentación durante la actualización. El equipo se reiniciará dos veces durante esta actualización.
14. Tras la actualización, en la primera pantalla de arranque antes de que Windows se inicie, verifique que aparece la versión 2.34 de la BIOS en la parte inferior izquierda de la pantalla.

OPCIONAL: Cómo instalar la mejora del rendimiento de INW Server

Los siguientes parches no solucionan ninguna vulnerabilidad de seguridad y son opcionales, aunque pueden mejorar el rendimiento de la red. Se debe seguir el procedimiento de instalación que se recoge a continuación, así como instalar todos los parches siguientes. Esta instalación puede tardar hasta 12 horas; la instalación de KB2775511 es la que consume la mayor parte de este tiempo.

1. Con un sistema no MLCL, visite las siguientes direcciones y descargue los parches en soportes portátiles.
   Visite http://catalog.update.microsoft.com/ e introduzca los números KB siguientes para acceder a los parches.
   KB2775511: http://support.microsoft.com/kb/2775511
   KB2732673: http://support.microsoft.com/kb/2732673
   KB2728738: http://support.microsoft.com/kb/2728738
   KB2878378: http://support.microsoft.com/kb/2878378

   Los parches siguientes se resumen en KB2473205: https://support.microsoft.com/en-us/kb/2473205
   KB2535094: http://support.microsoft.com/kb/2535094 Descargar de: https://support.microsoft.com/en-us/hotfix/kbhotfix?kbnum=2535094&kbln=en-us
   KB2914677: http://support.microsoft.com/kb/2914677 Descargar de: https://support.microsoft.com/en-us/hotfix/kbhotfix?kbnum=2914677&kbln=en-us
   KB2831013: http://support.microsoft.com/kb/2831013 Descargar de: https://support.microsoft.com/en-us/hotfix/kbhotfix?kbnum=2831013&kbln=en-us
   KB3000483: http://support.microsoft.com/kb/3000483 Descargar de: http://catalog.update.microsoft.com/
   KB3080140: http://support.microsoft.com/kb/3080140 Descargar de: http://catalog.update.microsoft.com/
   KB3044428: http://support.microsoft.com/kb/3044428 Descargar de: https://support.microsoft.com/en-us/hotfix/kbhotfix?kbnum=3044428&kbln=en-us

2. Inicie sesión en INW Server como **administrador**.
3. Introduzca el soporte portátil e instale los parches en el orden indicado con anterioridad.
4. Siga las instrucciones de instalación de Microsoft para completar la instalación de los parches.
5. Seleccione **Inicio de Windows -> Ejecutar** y acceda a **Regedit**.

6. En la ventana **Regedit**, vaya a **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Tcpip**.
7. En el menú del diálogo, seleccione **Archivo -> Exportar**. Cambie el nombre del archivo a **MLCLRegSave.reg** y colóquelo en el directorio **C:\Temp**.
8. En las ventanas Regedit, desde **Tcpip**, vaya hasta **Parámetros**.
9. En el menú del diálogo, seleccione **Editar -> Nuevo -> Valor de DWORD (32 bits)**. Se creará una entrada nueva; cámbiele el nombre a "**MaxUserPort**".
10. Haga clic con el botón derecho en "**MaxUserPort**", seleccione **Modificar** e introduzca el valor **65534** con una base de **Decimal**.
11. Siga el mismo procedimiento descrito con anterioridad y cree una entrada nueva con el nombre "**TcpTimedWaitDelay**". Introduzca el valor **60** con una base de **Decimal**.
12. Salga del diálogo **Regedit**.
13. Reinicie INW Server.

OPCIONAL: Cómo instalar el complemento 20007 - Deshabilitar SSL V2/V3 – KB187498

1. Inicie sesión en Windows como **Administrador** o un miembro de ese grupo.
2. Abra el indicador de comandos e introduzca los comandos siguientes:
3. REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0" /f
4. REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Client" /v DisabledByDefault /t REG_DWORD /d 00000001 /f
5. REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server" /v DisabledByDefault /t REG_DWORD /d 00000001 /f
6. REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server" /v Enabled /t REG_DWORD /d 00000000 /f
7. REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0" /f
8. REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server" /f
9. REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server" /v DisabledByDefault /t REG_DWORD /d 00000001 /f
10. REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server" /v Enabled /t REG_DWORD /d 00000000 /f
11. Cierre el indicador de comandos.

OPCIONAL: Cómo instalar el complemento 35291 – Weak Hashing

1) Cargue el certificado de seguridad de SQL Server en todos los sistemas ML/CL de la red (servidor, adquisiciones, revisiones y revisiones virtuales) o en la adquisición autónoma ML/CL.
2) Deshabilite el RDP en cada miembro de la red.
   a) Mi PC > Propiedades > Configuración remota > Remoto.
   b) Marque "No permitir las conexiones a este equipo".
   c) Haga clic en Aceptar y reinicie.

OPCIONAL: Cómo instalar el complemento 65821 – Conjuntos de cifrado compatibles SSL RC4

1. Inicie sesión en Windows como **Administrador** o un miembro de ese grupo.
2. Abra el indicador de comandos e introduzca los comandos siguientes:
3. REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 128/128" /f
4. REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 128/128" /v Enabled /t REG_DWORD /d 00000000 /f
5. REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 40/128" /f
6. REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 40/128" /v Enabled /t REG_DWORD /d 00000000 /f
7. REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128" /f
8. REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128" /v Enabled /t REG_DWORD /d 00000000 /f
9. Cierre el indicador de comandos.

OPCIONAL: Cómo eliminar la vulnerabilidad del complemento 63155 – Enumeración de rutas de servicio sin comillas de Microsoft Windows

1. Inicie sesión en Windows como Administrador o un miembro de ese grupo.
2. Para abrir Regedit, haga lo siguiente:
    a. En Windows 7:
        i. Vaya a HKLM\System\CurrentControlset\Services\RtkAudioService.
        ii. Cambie el valor de clave de la ruta de imagen de:
            C:\Program Files\Realtek\Audio\HDA\RtkAudioService.exe
            A:
            "C:\Program Files\Realtek\Audio\HDA\RtkAudioService.exe"
            Nota: Las comillas de apertura y cierre forman parte del valor de clave. Las comillas son lo que elimina la vulnerabilidad.

    b. En Windows 2008R2:
        i. Vaya a HKLM\System\CurrentControlset\Services\Gems Task Scheduler.
        ii. Cambie el valor de clave de la ruta de imagen de:
            C:\Program Files (x86)\GE Healthcare\MLCL\Bin\ArchiveUtility\GEMS_TaskSvc.exe
            A:
            "C:\Program Files (x86)\GE Healthcare\MLCL\Bin\ArchiveUtility\GEMS_TaskSvc.exe"
            Nota: Las comillas de apertura y cierre forman parte del valor de clave. Las comillas son lo que elimina la vulnerabilidad.

OPCIONAL: Cómo deshabilitar el protocolo SMB1

1. Inicie sesión en Windows como **Administrador** o un miembro de ese grupo.
2. Abra el indicador de comandos e introduzca los comandos siguientes:
3. REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" /f
4. REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" /v SMB1 /t REG_DWORD /d 00000000 /f
5. sc.exe config lanmanworkstation depend= bowser/mrxsmb20/nsi
6. sc.exe config mrxsmb10 start= disabled

Enlaces a los parches

Los parches que se muestran a continuación se han validado de manera independiente y pueden instalarse de forma individual, aunque se recomienda instalar todos los parches validados. En la lista de parches validados, hay dependencias. Se recomienda instalar los parches que se recogen en la tabla siguiente por orden, de arriba a abajo, con el fin de garantizar que se cumplen los requisitos previos de todos los parches. A veces, las dependencias de los parches requerirán que el sistema se reinicie; estos casos se identifican en las tablas siguientes.

NOTA: Debido a la configuración de los centros, al conjunto de parches del sistema, a los parches validados que se hayan instalado previamente o a las dependencias de los parches, existe la probabilidad de que algunos parches no puedan instalarse porque la funcionalidad ya esté instalada. El instalador de parches de Microsoft le avisará de este problema. En ese caso, continúe con la instalación del parche siguiente.

Ubicaciones alternativas de los parches: A principios de 2016, Microsoft anunció que algunos parches dejarían de estar disponibles en el Centro de descargas de Microsoft: https://blogs.technet.microsoft.com/msrc/2016/04/29/changes-to-security-update-links/. Por este motivo, es posible que no funcionen algunos de los enlaces que se recogen a continuación. Microsoft puede mover o eliminar estos enlaces en cualquier momento sin previo aviso. No obstante, si los enlaces no funcionan, existen dos métodos alternativos para descargar los parches. El primero es el Catálogo de Microsoft: http://catalog.update.microsoft.com. La mayor parte de las correcciones que no estén en el Centro de descargas de Microsoft estarán disponibles en el Catálogo de Microsoft. Si no se encuentra la corrección en el Catálogo, Microsoft cuenta con archivos ISO mensuales de las actualizaciones de seguridad disponibles en: https://support.microsoft.com/en-us/kb/913086. Para utilizar los archivos ISO, averigüe el mes del parche, descargue el archivo ISO pertinente y extraiga el parche. Si, después de haber recurrido a estos tres métodos, sigue sin conseguir un parche, póngase en contacto con el servicio de asistencia técnica de GE.

Rutas de instalación de 6.9.6

Hay varias rutas de instalación en función de la versión de 6.9.6 instalada y de cualquier parche anterior que se haya instalado. La información que se muestra a continuación le guiará hasta la ruta de instalación correcta.

Averigüe qué versión de 6.9.6 está utilizando. Puede comprobarlo en la aplicación Mac-Lab/CardioLab. Vaya a Ayuda/Acerca de y verá el número de versión. El número de versión, junto con el escenario de instalación, determinará la ruta correcta.

Nota: Las actualizaciones de seguridad opcionales de MLCL se pueden aplicar después de haber instalado todos los demás parches o actualizaciones. Las actualizaciones opcionales proporcionan seguridad adicional, pero no son obligatorias. Puede instalar algunos de los parches opcionales, pero elegir omitir otros. Por ejemplo, es posible que desee deshabilitar algunos de los protocolos vulnerables, pero no querer tratar la vulnerabilidad "Weak Hashing" debido al coste y a la complejidad de la gestión del certificado. Esta no causará problemas. Sin embargo, ***se recomienda encarecidamente la instalación de todas las demás actualizaciones***.

Algunas actualizaciones están documentadas como **reemplazadas**. Se han conservado en el documento, pero pueden omitirse.
Los escenarios de ejemplo siguientes se ofrecen para que el usuario los tenga como referencia.

(1) Configuración nueva/restablecimiento de imagen inicial de una máquina para recuperación ante desastres.
  (a) Para la R3, aplique las actualizaciones de la sección siguiente:
    (i) Actualizaciones 1 del parche de 2017 de MLCL V6.9.6

(2) La máquina se configuró y parcheó inicialmente, pero no se ha aplicado ninguna actualización posterior.
  (a) Para la R3, aplique las actualizaciones de la sección siguiente:
    (i) No se requieren más parches. Las actualizaciones del parche deberían haberse instalado como parte de la configuración.

(3) La máquina se configuró y todos los parches anteriores se han instalado.
  (a) Para la R3, aplique las actualizaciones de la sección siguiente:
    (i) No se requieren más parches. Las actualizaciones del parche deberían haberse instalado como parte de la configuración.

Parches sin validar de MLCL v6.9.6 R3

	INW Server	**Adquisición: Mac-Lab IT/XT/XTi, CardioLab IT/XT/XTi y SpecialsLab**	**GE Client Review Workstation**	**Virtual Review**
Plataforma del sistema operativo	**Windows Server 2008 R2 SP1**	**Windows 7 SP1**	**Windows 7 SP1**	**Windows 7 SP1**
Vulnerabilidad sin validar en la actualidad	KB4056897(CVE-2018-0747) HPESBHF03805 rev. 10 CP034007 KB4074587(CVE-2018-0847) HPSBHF03576 rev. 1	KB4056897(CVE-2018-0747) HPESBHF03805 rev. 10 KB4074587(CVE-2018-0847) HPSBHF03576 rev. 1	KB4056897(CVE-2018-0747) HPESBHF03805 rev. 10 KB4074587(CVE-2018-0847) HPSBHF03576 rev. 1	KB4056897(CVE-2018-0747) HPESBHF03805 rev. 10 KB4074587(CVE-2018-0847) HPSBHF03576 rev. 1

Actualizaciones 1 del parche de 2017 de MLCL V6.9.6

Windows 7 (Acquisition, Review y Virtual Review)		
KB	**Enlace**	**Notas**
	Realice el cambio de registro siguiente.	
	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing]	
	State=dword:00023c00	
KB2901907	https://www.microsoft.com/en-us/download/details.aspx?id=42642	Hacer clic con el botón derecho y Ejecutar como administrador.
Adobe 11.0.20	http://supportdownloads.adobe.com/thankyou.jsp?ftpID=6157&fileID=6191	
KB4025341 Paquete de actualizaciones de julio de 2017	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=12c93ad9-ef0e-4ce6-8a1d-84713223d24a	
KB4034664 Paquete de actualizaciones de agosto de 2017 **reemplazado**	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=e0a94bad-5b2c-4611-9066-24491ce9bb4f	Para instalar correctamente este paquete de actualizaciones, debe desinstalar el paquete de actualizaciones de julio **KB4025341 y reiniciar antes de instalar KB4034664**.
Reinicio necesario	-	
KB4019112	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=1daeb6d1-b103-4baa-bbde-5326e17e89e4	Ejecutar solo KB4014514 y KB4014504. Para KB4014514, hacer clic con el botón derecho y Ejecutar como administrador.

KB3125869	https://support.microsoft.com/en-us/help/3125869/ms15-124-vulnerability-in-internet-explorer-could-lead-to-aslr-bypass-december-16,-2015	Descargue e instale solamente "Activar la función de endurecimiento del controlador de excepciones de User32 en Internet Explorer".
KB2889841	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=bb220b30-6d01-4e57-8db6-3e492d6b65d3	-
KB3178688	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=322c28f5-349c-468a-ac94-901616f52372	
KB3178690	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=06e2c9fb-65b7-48f5-b6e2-58071f17f9bd	
KB3178687	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=726adfc6-4ac9-4409-bdab-2892b7058e78	
kb3141538	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=6be5e673-e3f6-4c8e-8834-732baf0eb5d3	
KB3191847	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=4b4bbe2b-a25d-4509-a069-f5efc227b4ad	
KB3191907	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=c8533f11-51f9-4f84-96d8-c619947cc7c0	
KB3118310	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=c59a1bb2-ff1f-427a-a8d7-2cab1cb3e7d1	
KB3191843	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=f715a81d-102d-416a-9a89-e9ebdace0a6d	
KB3191899	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=7698c63a-b85f-4647-bcb1-1be0256c3f43	
KB3203468	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=7a599998-ca41-4840-90ea-8143724e5c6a	Utilizar all-proof-en-us_.....cab.

KB3213624	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=3658f96e-a521-429d-a9a9-e70e30f5d830	
HPSBHF03557 Rev. 1	ftp://ftp.hp.com/pub/softpaq/sp80001-80500/sp80050.exe	No aplicable para Virtual Review.
Actualización de la BIOS de HP z440	https://support.hp.com/us-en/drivers/selfservice/hp-z440-workstation/6978828	
KB3118378	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=ae54ce3d-e321-4831-a1ba-fcae8eb430a0	
Reinicio necesario	-	
	Realice el cambio de registro siguiente.	
	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing]	
	State=dword:00010000	
Windows 2008R2 (INW)		
KB	Enlace	
	Realice el cambio de registro siguiente.	
	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing]	
	State=dword:00023c00	
Adobe 11.0.20	http://supportdownloads.adobe.com/thankyou.jsp?ftpID=6157&fileID=6191	
KB3125869	https://support.microsoft.com/en-us/help/3125869/ms15-124-vulnerability-in-internet-explorer-could-lead-to-aslr-bypass-december-16,-2015	Descargue e instale solamente "Activar la función de endurecimiento del controlador de excepciones de User32 en Internet Explorer".

KB4025341 Paquete de actualizaciones de julio de 2017	https://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=b2423c5b-0254-4747-88bb-ec1a785549cb	
Sustituido KB4034664 Paquete de actualizaciones de agosto de 2017	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=80f7899d-451d-4e3f-b54e-d488a06a3c58	Para instalar correctamente este paquete de actualizaciones, debe desinstalar el paquete de actualizaciones de julio **KB4025341 y reiniciar antes de instalar KB4034664**.
KB4019112	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=dedea6da-e039-487b-8ec6-2729551f7165	Ejecutar solo KB4014514 y KB4014504. Para KB4014514, hacer clic con el botón derecho y Ejecutar como administrador.
HPSBMU03653 rev.1	https://h20566.www2.hpe.com/hpsc/swd/public/detail?swItemId=MTX_083799d6dad34195bb47cb43c1	
Reinicio necesario		
	Realice el cambio de registro siguiente.	
	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing] **State=dword:00010000**	
	[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters] **LdapEnforceChannelBinding=DWORD:1**	Se aplican solo en el controlador de dominio Necesario el inicio del paquete de actualizaciones de julio - KB4025341 (CVE-2017-8563).

Actualizaciones 2 del parche de 2017 de MLCL V6.9.6

Los siguientes parches proporcionan al sistema MLCL parches más recientes y resuelven diferentes vulnerabilidades de seguridad. Se aplican las siguientes directrices:

1) Los parches mencionados anteriormente son los parches necesarios para 6.9.6 y deben instalarse en primer lugar.
2) Es probable que algunos de estos parches ya estén en el sistema.
3) Preste atención a la sección de notas para ver las instrucciones de manipulación especiales.
4) Los parches deben instalarse en orden, salvo que se especifique lo contrario.
5) Solo es necesario reiniciar si así se indica. Si un parche solicita el reinicio posterior, el sistema podrá reiniciarse, pero no es necesario.
6) Los parches no se instalarán si el componente de software sobre el que deben aplicarse no está presente (como un parche para IE8 en un sistema que no tiene instalado IE8).

Nota: KB4041681 sustituye a KB4041678 tanto en Windows 7 como en Windows Server 2008 R2 para resolver CVE-2017-11771, CVE-2017-11772, CVE-2017-11780 y CVE-2017-11781.

Windows 7 (Acquisition, Review y Virtual Review)		
KB	**Enlace**	**Notas**
	Realice el cambio de registro siguiente.	
	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing]	
	State=dword:00023c00	
Adobe 11.0.23	http://supportdownloads.adobe.com/thankyou.jsp?ftpID=6279&fileID=6314	
KB4041681 Octubre de 2017 Paquete de actualizaciones mensual	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=8a346e85-6ae3-46aa-a9e1-2e70e760f61c	

	Realice el cambio de registro siguiente.	
	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing]	
	State=dword:00010000	
	Reinicio necesario	

Windows 2008R2 (INW Server)

KB	Enlace	Notas
	Realice el cambio de registro siguiente.	
	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing]	
	State=dword:00023c00	
Adobe 11.0.23	http://supportdownloads.adobe.com/thankyou.jsp?ftpID=6279&fileID=6314	
	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=cd0388fd-5aca-4a13-8417-c28e1d8b7dda	**Para instalar correctamente este paquete de actualizaciones, debe desinstalar el paquete de actualizaciones de julio KB4025341, el paquete de actualizaciones de agosto KB4034664 y reiniciar antes de aplicar KB4041681.** Realice el cambio de registro siguiente – Solo en

KB4041681 Octubre de 2017 Paquete de actualizaciones mensual		el controlador de dominio si no existe: [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters] LdapEnforceChannelBinding=DWORD:1. **Esta clave de registro es necesaria en el controlador de dominio** que inicia el paquete de actualizaciones de julio - KB4025341 (CVE-2017-8563).
	Realice el cambio de registro siguiente.	
	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing] **State=dword:00010000**	
	Reinicio necesario	

Actualizaciones 3 del parche de 2018 de MLCL V6.9.6

Los siguientes parches proporcionan al sistema MLCL parches más recientes y resuelven diferentes vulnerabilidades de seguridad. Se aplican las siguientes directrices:

1) Los parches mencionados anteriormente son los parches necesarios para 6.9.6 y deben instalarse en primer lugar.
2) Preste atención a la sección de notas para ver las instrucciones de manipulación especiales.
3) Los parches deben instalarse en orden, salvo que se especifique lo contrario.
4) Solo es necesario reiniciar si así se indica. Si un parche solicita el reinicio posterior, el sistema podrá reiniciarse, pero no es necesario.
5) **Política de contraseñas:** La **longitud mínima de la contraseña** se puede cambiar por encima del límite de 14 caracteres para satisfacer sus requisitos de seguridad.

Siga estos pasos para realizar los siguientes cambios en el registro a fin de poner solución a las vulnerabilidades de los paquetes de actualización mensual de junio y septiembre.
Referencia: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8529

Windows 7 (Acquisition, Review y Virtual Review) y Windows 2008R2 (INW Server):

1. Haga clic en **Inicio**, **Ejecutar**, escriba **regedt32** o **regedit** y, a continuación, haga clic en **Aceptar**.
2. En el editor de registro, busque la siguiente carpeta del registro: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl**
3. Haga clic con el botón derecho en **FeatureControl**, coloque el puntero sobre **Nuevo** y, a continuación, haga clic en **Clave**.
4. Escriba **FEATURE_ENABLE_PRINT_INFO_DISCLOSURE_FIX** y, a continuación, pulse Intro para dar nombre a la nueva subclave.
5. Haga clic con el botón derecho en **FEATURE_ENABLE_PRINT_INFO_DISCLOSURE_FIX**, coloque el puntero sobre **Nuevo** y, a continuación, haga clic en **Valor de DWORD**.
6. Introduzca "iexplore.exe" como nuevo valor de DWORD.
7. Haga doble clic en el nuevo valor DWORD llamado "iexplore.exe" y cambie el campo de datos **Valor** a **1**.
8. Haga clic en **Aceptar** para cerrar.

Windows 2008R2 (INW Server):

1. Haga clic en **Inicio**, **Ejecutar**, escriba **regedt32** o **regedit** y, a continuación, haga clic en **Aceptar**.
2. En el editor de registro, busque la siguiente carpeta de registro: **HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Internet Explorer\Main\FeatureControl**
3. Haga clic con el botón derecho en **FeatureControl**, coloque el puntero sobre **Nuevo** y, a continuación, haga clic en **Clave**.
4. Escriba **FEATURE_ENABLE_PRINT_INFO_DISCLOSURE_FIX** y, a continuación, pulse Intro para dar nombre a la nueva subclave.
5. Haga clic con el botón derecho en **FEATURE_ENABLE_PRINT_INFO_DISCLOSURE_FIX**, coloque el puntero sobre **Nuevo** y, a continuación, haga clic en **Valor de DWORD**.
6. Introduzca "iexplore.exe" como nuevo valor de DWORD.
7. Haga doble clic en el nuevo valor DWORD llamado "iexplore.exe" y cambie el campo de datos **Valor** a **1**.
8. Haga clic en **Aceptar** para cerrar.

Windows 7 (Acquisition, Review y Virtual Review)		
KB	**Enlace**	**Notas**
	Realice el cambio de registro siguiente.	
	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing]	
	State=dword:00023c00	

KB4048957 Paquete de actualizaciones mensual de noviembre de 2017	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=224b07ab-de98-45f0-8b9c-83551cac66f6	
	Reinicio necesario	
KB4054518 Paquete de actualizaciones mensual de diciembre de 2017	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=5b48d1cb-83f7-43e1-9308-18872ffe4dce	
	Reinicio necesario	
KB3203468 Microsoft Office 2010 de julio de 2017	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=7a599998-ca41-4840-90ea-8143724e5c6a	
KB3213626 Microsoft Office 2010 de septiembre de 2017	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=2bb1487f-b287-41a9-b0ec-01b42aa4759e	
KB3128027 Microsoft PowerPoint 2010 de septiembre de 2017	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=474aa90a-7767-4f4f-b3f5-2ffa12fea4e6	

KB3141537 Microsoft Publisher 2010 de septiembre de 2017	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=0c646d3e-697d-4463-a6ea-afb3493c5cea	
KB2553338 Microsoft Office 2010 SP2 de octubre de 2017	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=14e73852-cbd2-456a-a9a8-7f0c10f1fa40	Es posible que se muestre un mensaje de error (No se puede instalar la ruta de la actualización...). Este mensaje de error se puede ignorar.
KB2837599 Microsoft Office 2010 SP2 de octubre de 2017	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=54ccbc02-879e-4aa1-b817-12418ce8dfcd	
KB4011612 Microsoft Office 2010 SP2 de diciembre de 2017	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=8230d598-8ab1-4efc-89b6-d3507a6dfd20	Es posible que se muestre un mensaje de error (No se puede instalar la ruta de la actualización...). Este mensaje de error se puede ignorar.
KB4011660 Microsoft Excel 2010 de enero de 2018	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=d7594745-04d5-4631-b2d7-289816f4dd43	
KB4011659 Microsoft Word 2010 de enero de 2018	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=0b5a1bf0-3043-47fd-afc3-d2fb55a46a96	

KB4011611 Microsoft Office 2010 SP2 de enero de 2018	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=3b2c376c-ea57-4925-b81d-3b765d456f2b	Coloque el parche en su equipo e inicie la extracción para instalarlo. Antes de dar por concluida la instalación, compruebe que las actualizaciones se han instalado.
KB4011610 Microsoft Office 2010 de enero de 2018	https://www.microsoft.com/en-us/download/details.aspx?id=56447	
KB4054172 .NET Framework de enero de 2018	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=537fc3ba-4248-40b8-9498-8a671abebfe9	Instale los siguientes parches: KB4054172, KB4019990 y KB4054176.
KB2719662	Cree las siguientes claves de registro.	
	Key=[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Windows\Sidebar\] **Value Name=[TurnOffSidebar]** **Type=[REG_DWORD]** **Data=[1]**	
KB2269637	Cree las siguientes claves de registro.	
	Key=[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\] **Value Name=[CWDIllegalInDllSearch]** **Type=[REG_DWORD]** **Data=[1]**	
	Realice el cambio de registro siguiente.	
	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing]	

	State=dword:00010000	
	Reinicio necesario	

Windows 2008R2 (INW Server)

KB	Enlace	Notas
	Realice el cambio de registro siguiente.	
	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing]	
	State=dword:00023c00	
KB3177467 Service Stack	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=f1b99598-a22d-4fbe-9b63-09724833acc3	**Necesario para instalar correctamente el paquete de actualizaciones mensual sin desinstalar el paquete de actualizaciones mensual previo.**
	Reinicio necesario	
KB4048957 Paquete de actualizaciones mensual de noviembre de 2017	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=435d3006-04ae-4c27-a5f9-3c36f09e58ed	
	Reinicio necesario	
KB4054518 Paquete de actualizaciones mensual de diciembre de 2017	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=09064e30-6f3e-4c99-8d09-fbc2ba06b436	

	Reinicio necesario	
KB4054172 .NET Framework de enero de 2018	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=fdecaf44-50a3-4667-a935-f9e7af0bb317	
KB2269637	Cree las siguientes claves de registro.	
	Key=[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\] **Value Name=[CWDIllegalInDllSearch]** **Type=[REG_DWORD]** **Data=[1]**	
	Realice el cambio de registro siguiente.	
	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing]	
	State=dword:00010000	
	Reinicio necesario	

Actualizaciones de seguridad opcionales de MLCL v6.9.6

Las siguientes actualizaciones opcionales pueden aplicarse para mejorar aún más el perfil de seguridad de los sistemas MLCL. Estas actualizaciones deben evaluarse en cada centro de conformidad con la política local de TI. Los cambios de configuración que se recogen en esta sección son compatibles con la funcionalidad del producto MLCL, pero pueden afectar a la infraestructura de TI específica de cada centro debido a la deshabilitación de los protocolos SSL heredados, lo que prohíbe el uso del escritorio remoto y requiere la generación y el mantenimiento de certificados.

	INW Server	**Adquisición: Mac-Lab IT/XT/XTi, CardioLab IT/XT/XTi y SpecialsLab**	**GE Client Review Workstation**	**Virtual Review**
Parche	**URL de descarga**	**URL de descarga**	**URL de descarga**	**URL de descarga**
MS16-047 KB3149090 reemplazado	https://technet.microsoft.com/library/security/MS16-047	https://technet.microsoft.com/library/security/MS16-047	https://technet.microsoft.com/library/security/MS16-047	https://technet.microsoft.com/library/security/MS16-047

	INW Server	Adquisición: Mac-Lab IT/XT/XTi, CardioLab IT/XT/XTi y SpecialsLab	GE Client Review Workstation	Virtual Review
Complemento 20007 – Deshabilitar SSL V2/V3 – KB187498	Consulte la sección "Cómo instalar el complemento 20007 - Deshabilitar SSL V2/V3 – KB187498".	Consulte la sección "Cómo instalar el complemento 20007 - Deshabilitar SSL V2/V3 – KB187498".	Consulte la sección "Cómo instalar el complemento 20007 - Deshabilitar SSL V2/V3 – KB187498".	Consulte la sección "Cómo instalar el complemento 20007 - Deshabilitar SSL V2/V3 – KB187498".
Complemento 78479 - Poodle	No se requiere ningún cambio. Con el paso anterior, se corrige este problema.	No se requiere ningún cambio. Con el paso anterior, se corrige este problema.	No se requiere ningún cambio. Con el paso anterior, se corrige este problema.	No se requiere ningún cambio. Con el paso anterior, se corrige este problema.
Complemento 35291 – Weak Hashing	Consulte la sección "Cómo instalar el complemento 35291 – Weak Hashing". (Consulte https://technet.microsoft.com/en-us/library/ms191192(v=sql.105).aspx para obtener más información).	Consulte la sección "Cómo instalar el complemento 35291 – Weak Hashing". (Consulte https://technet.microsoft.com/en-us/library/ms191192(v=sql.105).aspx para obtener más información).	Consulte la sección "Cómo instalar el complemento 35291 – Weak Hashing". (Consulte https://technet.microsoft.com/en-us/library/ms191192(v=sql.105).aspx para obtener más información).	Consulte la sección "Cómo instalar el complemento 35291 – Weak Hashing". (Consulte https://technet.microsoft.com/en-us/library/ms191192(v=sql.105).aspx para obtener más información).
Complemento 45411	No se requiere ningún cambio. Con el paso anterior, se corrige este problema.	No se requiere ningún cambio. Con el paso anterior, se corrige este problema.	No se requiere ningún cambio. Con el paso anterior, se corrige este problema.	No se requiere ningún cambio. Con el paso anterior, se corrige este problema.
Complemento 65821 – Conjuntos de cifrado compatibles SSL RC4 (Bar Mitzvah)	Consulte la sección "Cómo instalar el complemento 65821 – Conjuntos de cifrado compatibles SSL RC4 (Bar Mitzvah)".	Consulte la sección "Cómo instalar el complemento 65821 – Conjuntos de cifrado compatibles SSL RC4 (Bar Mitzvah)".	Consulte la sección "Cómo instalar el complemento 65821 – Conjuntos de cifrado compatibles SSL RC4 (Bar Mitzvah)".	Consulte la sección "Cómo instalar el complemento 65821 – Conjuntos de cifrado compatibles SSL RC4 (Bar Mitzvah)".
Complemento 63155 – Enumeración de rutas de servicio sin comillas de Microsoft Windows	Consulte la sección "Cómo eliminar la vulnerabilidad del complemento 63155 – Enumeración de rutas de servicio sin comillas de Microsoft Windows".	Consulte la sección "Cómo eliminar la vulnerabilidad del complemento 63155 – Enumeración de rutas de servicio sin comillas de Microsoft Windows".	Consulte la sección "Cómo eliminar la vulnerabilidad del complemento 63155 – Enumeración de rutas de servicio sin comillas de Microsoft Windows".	Consulte la sección "Cómo eliminar la vulnerabilidad del complemento 63155 – Enumeración de rutas de servicio sin comillas de Microsoft Windows".

	INW Server	Adquisición: Mac-Lab IT/XT/XTi, CardioLab IT/XT/XTi y SpecialsLab	GE Client Review Workstation	Virtual Review
Complemento 59915 – Vulnerabilidades en los gadgets podrían permitir la ejecución remota de código	N/D	Siga la sección "**Disable the Sidebar in the system Registry**" (Deshabilite Sidebar en el Registro del sistema) del artículo siguiente: https://technet.microsoft.com/library/security/2719662.	Siga la sección "**Disable the Sidebar in the system Registry**" (Deshabilite Sidebar en el Registro del sistema) del artículo siguiente: https://technet.microsoft.com/library/security/2719662.	Siga la sección "**Disable the Sidebar in the system Registry**" (Deshabilite Sidebar en el Registro del sistema) del artículo siguiente: https://technet.microsoft.com/library/security/2719662.
Deshabilitar el protocolo SMB1	Consulte la sección "Cómo deshabilitar el protocolo SMB1".	Consulte la sección "Cómo deshabilitar el protocolo SMB1".	Consulte la sección "Cómo deshabilitar el protocolo SMB1".	Consulte la sección "Cómo deshabilitar el protocolo SMB1".

Política de contraseñas

Política de contraseñas: La longitud mínima de la contraseña se puede cambiar por encima del límite de 14 caracteres para satisfacer sus requisitos de seguridad. Consulte la sección **Contraseña** de la Guía de seguridad para obtener más información sobre el cambio de contraseñas.

Información de contacto

Si tiene más preguntas, póngase en contacto con el servicio de asistencia técnica.