GE Healthcare

Site Web Invasive Cardiology Security

Cardiologie interventionnelle - invasive

Groupe de produits :	Produits interventionnels invasifs
Produits :	Mac-Lab IT/XT/XTi, CardioLab IT/XT/XTi, SpecialsLab et ComboLab IT/XT/XTi systèmes d'enregistrement, systèmes de gestion des données Centricity Cardiology
Version :	6.9.6 Version 3
Objet :	Consignes de sécurité
Date :	9 mars 2018

Récapitulatif

Les informations suivantes sont fournies aux clients GE Healthcare Technologies en ce qui concerne les vulnérabilités de sécurité technique connues liées à Mac-Lab® Hemodynamic, CardioLab® Electrophysiology, SpecialsLab et les systèmes d'enregistrement ComboLab IT pour Cath Lab, EP Lab et d'autres laboratoires d'intervention ainsi que les systèmes de gestion des données de cardiologie Centricity®.

Configuration de base de correctifs de sécurité

La configuration de base de correctifs de sécurité des systèmes Mac-Lab IT/XT/XTi et CardioLab il/XT/XTi au moment de la sortie est indiquée dans la configuration de base MLCL, à la section Hemodynamic, Electrophysiology and Cardiovascular Information Technologies du site Web http://www3.gehealthcare.com/en/Support/Invasive_Cardiology_Product_Security.

Processus

Les actions suivantes sont effectuées à chaque fois que Microsoft ou autres fabricants publient de nouveaux correctifs de sécurité :

- L'équipe d'ingénierie de cardiologie invasive effectue un processus d'analyse de sécurité sur le matériel et les logiciels pris en charge par Mac-Lab IT/XT/XTi, CardioLab IT/XT/XTi, GE Client Review et le serveur INW.
- Si une vulnérabilité répond aux critères de validation de Mac-Lab IT/XT/XTi et CardioLab IT/XT/XTi, la vulnérabilité est communiquée par le biais de la base de données de sécurité produit GEHC et le site Web Invasive Cardiology Security dans les trois semaines suivant la sortie de la version du correctif.

- Dès la validation de la vulnérabilité Mac-Lab IT/XT/XTi et CardioLab IT/XT/XTi, les instructions d'installation de la base de données de sécurité produit GEHC, du site Web Invasive Cardiology Security et du Mac-Lab IT/XT/XTi et CardioLab IT/XT/XTi atteints sont mises à jour.

Les critères de validation de vulnérabilité du Mac-Lab IT/XT/XTi et du CardioLab IT/XT/XTi sont comme suit : toute vulnérabilité qui permet aux logiciels malveillants de modifier ou de refuser les fonctionnalités Mac-Lab IT/XT/XTi et CardioLab IT/XT/XTi et/ou d'infecter et se propager par une utilisation normale du système.

Les clients doivent rester informés par les notifications en vulnérabilité de Microsoft et visiter les sites Web de cardiologie invasive pour comprendre l'impact sur Mac-Lab IT/XT/XTi et CardioLab IT/XT/XTi. Une fois qu'un correctif de sécurité est validé, les clients sont responsables de son installation. Toutes les instructions d'installation des correctifs de sécurité pour Mac-Lab IT/XT/XTi et CardioLab IT/XT/XTi sont disponibles sur le site Web Invasive Cardiology Security sous le tableau des correctifs validés.

Les vulnérabilités exposées après la sortie produit Mac-Lab IT/XT/XTi et CardioLab IT/XT/XTi qui ne répondent pas aux critères pour être validées ne sont pas énumérés dans base de données de sécurité produit GEHC et le site Web Invasive Cardiology Security. Ces vulnérabilités sont considérées comme non-critiques et/ou en dehors du flux de travail clinique des systèmes Mac-Lab IT/XT/XTi, CardioLab IT/XT/XTi et Centricity INW et ne seront pas validées. Les correctifs non répertoriés ne doivent pas être installés sur les produits afin d'éliminer les risques de dysfonctionnement et de panne.

CONTENU

Historique des révisions

Révision	Date	Commentaires
1.0	22 septembre 2017	• 6.9.6 Séparation de document • B4025341qualifié - Rollup mensuel juillet • Chemins d'installation 6.9.6 ajoutés pour simplifier l'installation des correctifs • Correctifs non qualifiés de septembre
2.0	13 octobre 2017	• Instructions ajoutées pour désactiver le protocole SMB1
3.0	27 octobre 2017	• Correctifs non qualifiés d'octobre
4.0	20 novembre 2017	• Correctifs qualifiés d'octobre ajoutés
5.0	11 décembre 2017	• Correctifs non qualifiés de novembre
6.0	20 décembre 2017	• Pour le correctif mensuel d'octobre, consignes ajoutées pour désinstaller les correctifs mensuels précédents avant l'installation du correctif mensuel d'octobre sur le serveur
7.0	26 janvier 2018	• Rollups qualifiés mensuels de novembre et décembre avec d'autres correctifs. Correctifs non qualifiés de janvier également ajoutés
8.0	9 mars 2018	• Correctif non qualifié de février ajouté • Modifications qualifiées de la longueur minimale du mot de passe • Verbiage modifié de « Actualisation de correctif » en « Mises à jour de correctif » • Recommandations supplémentaires sur la sécurité des systèmes MLCL

Recommandations supplémentaires sur la sécurité des systèmes MLCL

Nous vous recommandons de suivre ces recommandations ainsi que les recommandations présentées dans le Guide de sécurité MLCL.

- Mise en œuvre de stratégies solides de mots de passe et de gestion de comptes
- Modification du mot de passe par défaut par un mot de passe unique, plus fort et plus sûr pour les comptes d'utilisateur
- Instauration de zones démilitarisées et défenses de périmètre pour le réseau du site
- Pare-feu réseau
- Blocage de l'accès Internet sur les systèmes MLCL

- Systèmes de détection d'intrusion - système de protection d'intrusion réseau
- Réseaux privés virtuels
- Analyse de trafic réseau
- Renforcement de la sécurité physique
- Analyse des journaux
- Suivre la section Mises à jour de sécurité MLCL v6.9.6 facultatives

Installation des correctifs de sécurité sur les systèmes MLCL

Configurations requises :

- Les mises à jour peuvent s'appliquer à tout moment sauf quand l'application Mac-Lab IT/XT/XTi, CardioLab IT/XT/XTi ou SpecialsLab est ouverte.
- Les mises à jour doivent être réappliquées si le système est ré-imagé.
- Les mises à jour s'appliquent à la fois aux systèmes en réseau et autonomes.
- La meilleure pratique consiste à mettre à jour tous les systèmes MLCL applicables sur site.

Ce document s'applique à 6.9.6R3 uniquement. Veuillez vérifier que vous exécutez bien 6.9.6 en utilisant la procédure suivante avant de continuer :

1. Lancez l'application Mac-Lab CardioLab.
2. Sélectionnez ***Help*** > ***About Mac-Lab*** (Aide > À propos de Mac-Lab) (ou ***CardioLab***, le cas échéant).
3. Vérifiez que le numéro de version est bien **6.9.6 Version 3**.
4. Cliquez sur ***Close*** (Fermer).
5. Fermez l'application.

Recommandations : utilisez Internet Explorer (IE) pour télécharger le catalogue. Si vous utilisez le panier pour télécharger des correctifs, vous devez ouvrir un autre onglet ou une nouvelle fenêtre http://catalog.update.microsoft.com **pour voir le contenu du panier.**

Procédure de connexion aux systèmes d'acquisition et d'examen

Lors du démarrage du système d'acquisition et d'examen Mac-Lab, CardioLab ou SpecialsLab, une séquence de connexion automatique commence et se connecte automatiquement au système d'exploitation. Pour installer un correctif de sécurité, l'utilisateur doit être connecté comme **mlcltechuser**.

REMARQUE : le mot de passe est contenu dans le manuel de sécurité. Sinon, contactez l'administrateur système ou le support technique GE pour obtenir le mot de passe actuel.

1. Mise sous tension du système d'acquisition.
2. Le système démarre avec la fenêtre ***d'identification personnalisée***.
3. Appuyez sur **Ctrl + Alt + Suppr**.
4. Cliquez sur ***Logoff*** (Déconnexion). Sur Windows XP, cliquez sur ***Logoff*** (Déconnecter) à nouveau.
5. Cliquez sur ***OK***.
6. Maintenez immédiatement la touche **Maj.** jusqu'à ce que la page de connexion s'affiche.
7. Connectez-vous localement au système d'exploitation **mlcltechuser**.
8. Connectez-vous localement à la fenêtre ***d'identification personnalisée*** en tant que **mlcltechuser**.

Comment se connecter au serveur Centricity Cardiology INW

Le mot de passe est contenu dans le manuel de sécurité. Sinon, contactez l'administrateur système ou le support technique GE pour obtenir le mot de passe actuel. Connectez-vous au serveur INW en tant qu'**administrateur**.

Comment se connecter aux systèmes MLCL logiciel seul

Puisque les systèmes logiciel seul sont pris en charge par le client, le système doit être connecté avec un compte **administrateur**.

Comment installer un micrologiciel d'imprimante

Le système qui appliquera le micrologiciel de l'imprimante doit être fourni par le client.
REMARQUE : le système Mac-Lab CardioLab ne doit pas être utilisé pour télécharger et/ou appliquer le micrologiciel de l'imprimante.

- Suivez le lien de téléchargement dans le tableau.
- Sélectionnez l'imprimante appropriée.
- Sélectionnez Français et le système d'exploitation MLCL applicable.
- Sélectionnez Français et dans la catégorie Micrologiciel sélectionnez l'utilitaire de mise à jour du micrologiciel applicable et cliquez sur Download (Télécharger).
- Lancez l'installation du micrologiciel et suivez les instructions complètes pour terminer la mise à jour du micrologiciel.

Comment mettre à jour Intel Management Engine Firmware (HP Z440) – HPSBHF03557 Rév. 1

1. Connectez-vous au SE Windows et à la fenêtre ***d'identification personnalisée*** MLCL en tant que **mlcltechuser**.
2. Accédez à l'emplacement à l'intérieur de la section *MLCL V6.9.6 Mises à jour de correctif*, qui contient le fichier de mise à jour Intel Management Engine **sp80050.exe**.
3. Faites un clic droit sur **sp80050.exe** et sélectionnez ***Run as administrator*** (Exécuter en tant qu'administrateur).
4. Cliquez sur ***Yes*** (Oui) dans la boîte de dialogue User Account Control (Contrôle de compte d'utilisateur).
5. Cliquez sur ***Next*** (Suivant) dans l'assistant Install Shield.
6. Acceptez le contrat de licence et cliquez sur ***Next*** (Suivant).
7. Appuyez sur **Y** à l'invite de commande « Do you want to update the Management Engine Firmware now [Y/N] ?» (Voulez-vous mettre à jour le micrologiciel de gestion de moteur maintenant [O/N] ?).
8. Redémarrez le système une fois la mise à jour du micrologiciel terminée.

Mesures pour vérifier que la mise à jour du micrologiciel a réussi :

1. Après le redémarrage du système, à l'intérieur de l'écran HP appuyez sur **F10** pour accéder au menu de configuration.
2. Allez sur ***Main > System Information*** (Principal > Informations système).
3. La version du micrologiciel ME doit être ***9.1.41.3024***.

Instructions de mise à jour de Z440 BIOS à v2.34 :

1. Rendez-vous à la section Assistance clientèle HP - Site Web de téléchargement de logiciels et pilotes :

   https://support.hp.com/us-en/drivers/selfservice/hp-z440-workstation/6978828
2. Sélectionnez ***BIOS***.
3. Sélectionnez ***Download*** (Télécharger) pour HP Z440/Z640/Z840 Workstation System BIOS 2.34 Rev.A.
4. Connectez-vous à l'ordinateur z440 en tant qu'***administrateur***.
5. Exécutez le fichier téléchargé ***sp80745.exe***.
6. Sélectionnez ***Yes*** (Oui) pour autoriser.
7. Sélectionnez ***I accept the terms in the license agreement*** (J'accepte les termes du contrat de licence).
8. Sélectionnez ***View Contents of the HPBIOSUPDREC folder*** (Afficher le contenu du dossier HPBIOSUPDREC). Cela ouvre le dossier :

   C:\\swsetup\SP80745\HPBIOSUPDREC

9. Exécutez ***HPBIOSUPDREC.exe***.
10. Sélectionnez ***Yes*** (Oui) pour autoriser.
11. Après plusieurs secondes, un fichier journal est créé et une fenêtre d'utilitaire d'installation apparaît. Sélectionnez ***Update*** (Mettre à jour) et ***Next*** (Suivant).
12. Suivez les instructions à l'écran, sélectionnez ***Restart*** (Redémarrer).
13. La mise à jour du BIOS ne prendra que quelques minutes, ne coupez pas l'alimentation pendant la mise à jour. L'ordinateur va redémarrer deux fois au cours de cette mise à jour.
14. Après la mise à jour, sur le premier écran de démarrage avant que Windows se lance, vérifiez que la version 2.34 du BIOS apparaît en bas à gauche de l'écran.

FACULTATIF - Comment installer l'amélioration des performances du serveur INW

Les correctifs suivants ne permettent pas de résoudre les problèmes de sécurité et sont en option. Ces correctifs peuvent améliorer les performances du réseau. La procédure d'installation ci-dessous doit être suivie et tous les correctifs déployés ensemble. Ce déploiement peut prendre jusqu'à 12 heures, le grand pourcentage au sein de l'installation KB2775511.

1. À l'aide d'un système non MLCL, consultez et téléchargez les correctifs suivants sur un support amovible.
   Visitez la page http://catalog.update.microsoft.com/ et entrez ci-dessous les numéros KB pour accéder aux correctifs.
   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

   Les correctifs suivants sont répertoriés dans l'article suivant : KB2473205 - https://support.microsoft.com/en-us/kb/2473205
   KB2535094 – http://support.microsoft.com/kb/2535094 Téléchargement sur - https://support.microsoft.com/en-us/hotfix/kbhotfix?kbnum=2535094&kbln=en-us
   KB2914677 – http://support.microsoft.com/kb/2914677 Téléchargement sur - https://support.microsoft.com/en-us/hotfix/kbhotfix?kbnum=2914677&kbln=en-us
   KB2831013 – http://support.microsoft.com/kb/2831013 Téléchargement sur - https://support.microsoft.com/en-us/hotfix/kbhotfix?kbnum=2831013&kbln=en-us
   KB3000483 – http://support.microsoft.com/kb/3000483 Téléchargement sur - http://catalog.update.microsoft.com/
   KB3080140 – http://support.microsoft.com/kb/3080140 Téléchargement sur - http://catalog.update.microsoft.com/
   KB3044428 – http://support.microsoft.com/kb/3044428 Téléchargement sur - https://support.microsoft.com/en-us/hotfix/kbhotfix?kbnum=3044428&kbln=en-us

2. Connectez-vous au serveur INW en tant qu'**administrateur**.
3. Insérez le support amovible et installez les correctifs dans l'ordre indiqué ci-dessus.
4. Suivez les instructions d'installation de Microsoft pour terminer l'installation des correctifs.

5. Sélectionnez **Windows Start -> Run** (Démarrer - > Exécuter), tapez **Regedit** et Entrée.
6. Dans la fenêtre **Regedit**, accédez à **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Tcpip**
7. Dans la boîte de dialogue Menu, sélectionnez **File -> Export** (Fichier - > Exporter). Nommez le fichier **MLCLRegSave.reg** et placez-le dans le répertoire **C:\Temp**.
8. Dans la fenêtre Regedit, à partir de **tcpip** accédez aux **Paramètres**.
9. Dans la boîte de dialogue Menu, sélectionnez **Edit -> New -> DWORD (32-bit) Value** (Modifier - > Nouveau - > Valeur DWORD [32 bits]). Une nouvelle entrée est créée, nommez-la **"MaxUserPort"**.
10. Cliquez à droite sur **"MaxUserPort"**, sélectionnez **Modify** (Modifier) et entrez la valeur **65534** avec une base **Décimale.**
11. Suivez la même procédure ci-dessus et créez une nouvelle entrée nommée **'TcpTimedWaitDelay'.** Entrez la valeur **60** avec une base **Décimale**.
12. Quittez la boîte de dialogue **Regedit**.
13. Redémarrez le serveur INW.

FACULTATIF - Comment installer le plug-in 20007 - Désactiver SSL V2/V3 - KB187498

1. Connectez-vous en tant qu'**administrateur** ou membre de ce groupe.
2. Ouvrez une invite de commande et entrez les commandes suivantes :
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. Fermez l'invite de commande.

FACULTATIF - Comment installer le plug-in 35291 - Hachage faible

1) Chargez votre certificat de sécurité dans le serveur SQL sur chaque système ML/CL dans le réseau (serveur, acquisitions, évaluations et examens virtuels) ou acquisition ML/CL autonome.
2) Désactivez le RDP sur chaque membre du réseau.
   a) Mon Ordinateur >Propriétés >Paramètres >À distance
   b) Cochez l'option « Ne pas autoriser les connexions à cet ordinateur ».
   c) Cliquez sur OK et redémarrez.

FACULTATIF - Comment installer le plug-in 65821 - Suites de chiffrement SSL RC4 prises en charge

1. Connectez-vous en tant qu'**administrateur** ou membre de ce groupe.
2. Ouvrez une invite de commande et entrez les commandes suivantes :
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. Fermez l'invite de commande.

FACULTATIF - Comment supprimer une vulnérabilité pour le plug-in 63155 - Énumération de chemin d'accès du service Microsoft Windows sans guillemets

1. Connectez-vous en tant qu'administrateur ou membre de ce groupe.
2. Ouvrez Regedit pour effectuer les actions suivantes :
    a. Sous Windows 7
        i. Accédez à HKLM\System\CurrentControlset\Services\RtkAudioService
        ii. Remplacez la valeur de la clé du chemin d'accès de l'image :
            C:\Program Files\Realtek\Audio\HDA\RtkAudioService.exe
            par :
            "C:\Program Files\Realtek\Audio\HDA\RtkAudioService.exe"
            Remarque : les guillemets avant et arrière font partie de la valeur de la clé. Les guillemets permettent de supprimer la vulnérabilité.

    b. Sous Windows 2008R2
        i. Accédez à HKLM\System\CurrentControlset\Services\Gems Task Scheduler
        ii. Remplacez la valeur de la clé du chemin d'accès de l'image :
            C:\Program Files (x86)\GE Healthcare\MLCL\Bin\ArchiveUtility\GEMS_TaskSvc.exe
            par :
            "C:\Program Files (x86)\GE Healthcare\MLCL\Bin\ArchiveUtility\GEMS_TaskSvc.exe"
            Remarque : les guillemets avant et arrière font partie de la valeur de la clé. Les guillemets permettent de supprimer la vulnérabilité.

FACULTATIF - Comment désactiver le protocole SMB1

1. Connectez-vous en tant qu'**administrateur** ou membre de ce groupe.
2. Ouvrez une invite de commande et entrez les commandes suivantes :
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

Liens de correctifs

Les correctifs affichés ci-dessous sont qualifiés sur une base indépendante et peuvent être installés sur une base individuelle, bien qu'il soit recommandé d'installer tous les correctifs. Il existe des dépendances au sein de la liste de correctifs. Dans le tableau ci-dessous, il est recommandé d'installer les correctifs dans l'ordre (du haut vers le bas) afin de s'assurer que tous les prérequis sont respectés pour tous les correctifs. À l'occasion, les dépendances de correctifs nécessitent le redémarrage du système (indiqué dans le tableau ci-dessous).

REMARQUE : en raison des configurations du site, l'ensemble des correctifs du système, les correctifs qui ont déjà été installés ou les dépendances de correctifs, certains correctifs pourraient ne pas s'installer en raison d'une fonctionnalité déjà installée. L'installeur de correctifs Microsoft vous avertit de ce problème. Si cela se produit, veuillez continuer avec l'installation de correctif suivante.

Emplacements alternatifs de correctifs : au début de 2016 Microsoft a annoncé que certains correctifs ne seraient plus disponibles dans le Centre de téléchargement Microsoft https://blogs.technet.microsoft.com/msrc/2016/04/29/changes-to-security-update-links/ Par conséquent, certains des liens fournis ci-dessous peuvent ne pas fonctionner. Microsoft peut déplacer/supprimer ces liens à tout moment sans préavis. Cependant, si les liens ne fonctionnent pas, il existe deux autres méthodes pour le téléchargement des correctifs. La première est le catalogue Microsoft http://catalog.update.microsoft.com. La plupart des correctifs qui ne sont pas dans le centre de téléchargement Microsoft sont disponibles à partir du Catalogue Microsoft. Si un correctif n'est pas disponible dans le catalogue Microsoft, Microsoft dispose de fichiers ISO mensuels de mise à jour de sécurité disponibles à l'adresse suivante : https://support.microsoft.com/en-us/kb/913086 Pour utiliser les ISO, déterminez le mois du correctif, téléchargez l'ISO applicable et extrayez le correctif. Si après avoir essayé les trois méthodes vous n'obtenez toujours pas de correctif, veuillez contacter le Support Technique GE pour plus d'aide.

Chemins d'installation 6.9.6

Il existe plusieurs chemins d'installation en fonction de la version de 6.9.6 installée et des correctifs installés précédemment. Les renseignements suivants vous guideront vers le chemin d'installation correct.

Déterminez la version du 6.9.6 que vous exécutez. Aidez-vous pour cela de l'application Mac Lab/Cardio Lab. Rendez-vous dans la section Aide/À propos et vous verrez le numéro de version. Le numéro de version associé au scénario d'installation détermine le chemin correct.

Remarque : la section MLCL Optional Security Updates (Mises à jour de sécurité en option MLCL) peut être appliquée une fois tous les autres correctifs / toutes les mises à jour appliqué(e)s. Les mises à jour facultatives fournissent une sécurité supplémentaire, mais ne sont pas nécessaires. Vous pouvez appliquer certains des correctifs facultatifs, mais choisir d'en ignorer d'autres. Par exemple, vous pouvez choisir de désactiver certains des protocoles vulnérables ou de ne pas activer le hachage faible en raison des coûts et de la complexité de la gestion des certificats. Cela ne causera aucun problème. Cependant, ***toutes les autres mises à jour sont fortement recommandées***.

Certaines mises à jour sont documentées comme **remplacées**. Celles-ci sont laissées dans le document à des fins d'intégralité, mais peuvent être ignorées.
Les exemples de scénarios suivants sont fournis à titre de référence.

(1) Nouvelle configuration/re-imagerie d'une machine pour une reprise après sinistre.
  (a) Pour R3, appliquez les mises à jour de la section suivante
    (i) MLCL V6.9.6 2017 Mises à jour de correctif 1

(2) La machine a été installée et corrigée au départ, mais aucune autre mise à jour n'a été appliquée.
  (a) Pour R3, appliquez les mises à jour de la section suivante
    (i) Aucun autre correctif n'est nécessaire. Les mises à jour de correctif auraient été appliquées dans le cadre de l'installation

(3) La machine a été installée et tous les correctifs précédents ont été appliqués.
  (a) Pour R3, appliquez les mises à jour de la section suivante
    (i) Aucun autre correctif n'est nécessaire. Les mises à jour de correctif auraient été appliquées dans le cadre de l'installation

Correctifs non qualifiés MLCL v6.9.6 R3

	Serveur INW	**Acquisition - Mac-Lab IT/XT/XTi, CardioLab IT/XT/XTi et SpecialsLab**	**Poste de travail client GE de consultation**	**Revue virtuelle**
Plate-forme de système d'exploitation	**Windows Server 2008 R2 SP1**	**Windows 7 SP1**	**Windows 7 SP1**	**Windows 7 SP1**
Vulnérabilité non qualifiée actuelle	KB4056897(CVE-2018-0747) HPESBHF03805 rév.10 CP034007 KB4074587(CVE-2018-0847) HPSBHF03576 rév. 1	KB4056897(CVE-2018-0747) HPESBHF03805 rév.10 KB4074587(CVE-2018-0847) HPSBHF03576 rév. 1	KB4056897(CVE-2018-0747) HPESBHF03805 rév.10 KB4074587(CVE-2018-0847) HPSBHF03576 rév. 1	KB4056897(CVE-2018-0747) HPESBHF03805 rév.10 KB4074587(CVE-2018-0847) HPSBHF03576 rév. 1

MLCL V6.9.6 2017 Mises à jour de correctif 1

Windows 7 (Acquisition, examen et examen virtuel)		
KB	**Lien**	**Remarques**
	Effectuez le changement de registre suivant	
	[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	Effectuez un clic droit et exécutez en tant qu'administrateur
Adobe 11.0.20	http://supportdownloads.adobe.com/thankyou.jsp?ftpID=6157&fileID=6191	
KB4025341 Rollup de juillet 2017	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=12c93ad9-ef0e-4ce6-8a1d-84713223d24a	
KB4034664 Rollup d'août 2017 **Remplacé**	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=e0a94bad-5b2c-4611-9066-24491ce9bb4f	Pour installer ce rollup, désinstallez le rollup de juillet **KB4025341, puis redémarrez le système avant d'installer KB4034664**
Redémarrage requis	-	
KB4019112	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=1daeb6d1-b103-4baa-bbde-5326e17e89e4	Exécutez KB4014514 et KB4014504 uniquement. Pour KB4014514, effectuez un clic droit et exécuter en tant qu'administrateur

KB3125869	https://support.microsoft.com/en-us/help/3125869/ms15-124-vulnerability-in-internet-explorer-could-lead-to-aslr-bypass-december-16,-2015	Téléchargez et installez uniquement « Activer la fonctionnalité de durcissement du gestionnaire d'exceptions de User32 dans 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	Utilisez all-proof-en-us_.....cab

KB3213624	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=3658f96e-a521-429d-a9a9-e70e30f5d830	
HPSBHF03557 Rév. 1	ftp://ftp.hp.com/pub/softpaq/sp80001-80500/sp80050.exe	Non applicable pour l'examen virtuel.
Mise à jour du BIOS 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	
Redémarrage requis	-	
	Effectuez le changement de registre suivant	
	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing]	
	State=dword:00010000	
Windows 2008R2 (INW)		
KB	Lien	
	Effectuez le changement de registre suivant	
	[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	Téléchargez et installez uniquement « Activer la fonctionnalité de durcissement du gestionnaire d'exceptions de User32 dans Internet Explorer »

KB4025341 Rollup de juillet 2017	https://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=b2423c5b-0254-4747-88bb-ec1a785549cb	
KB4034664 **Remplacé** Rollup d'août 2017	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=80f7899d-451d-4e3f-b54e-d488a06a3c58	Pour installer ce rollup, désinstallez le rollup de juillet **KB4025341, puis redémarrez le système avant d'installer KB4034664**
KB4019112	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=dedea6da-e039-487b-8ec6-2729551f7165	Exécutez KB4014514 et KB4014504 uniquement. Pour KB4014514, effectuez un clic droit et exécuter en tant qu'administrateur
HPSBMU03653 rev.1	https://h20566.www2.hpe.com/hpsc/swd/public/detail?swItemId=MTX_083799d6dad34195bb47cb43c1	
Redémarrage requis		
	Effectuez le changement de registre suivant	
	[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**	Concerne uniquement le contrôleur de domaine Nécessite le démarrage du rollup de juillet KB4025341 (CVE-2017-8563)

MLCL V6.9.6 2017 Mises à jour de correctif 2

Les correctifs suivants actualisent le niveau de correctifs du système MLCL et résolvent plusieurs vulnérabilités de sécurité. Les directives suivantes s'appliquent :

1) Les correctifs ci-dessus sont des correctifs requis pour 6.9.6 et doivent être appliqués en premier.
2) Il est prévu que certains correctifs énumérés seront déjà sur le système.
3) Faites attention à la section Notes d'instructions particulières de manipulation.
4) Les correctifs doivent être appliqués dans l'ordre, sauf dans les cas indiqués.
5) Les redémarrages ne sont obligatoires que quand c'est précisé. Si un correctif nécessite un redémarrage à un autre moment, le système peut être redémarré, mais ce n'est pas nécessaire.
6) Les correctifs ne s'installent pas si le composant logiciel à corriger n'est pas présent (par exemple un correctif IE8 sur un système où IE8 n'est pas installé).

Remarque : KB4041681 remplace KB4041678 pour Windows 7 et Windows Server 2008 R2 pour corriger CVE-2017-11771, CVE-2017-11772, CVE-2017-11780 et CVE-2017-11781.

Windows 7 (Acquisition, examen et examen virtuel)		
KB	**Lien**	**Remarques**
	Effectuez le changement de registre suivant	
	[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 Octobre 2017 Rollup mensuel	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=8a346e85-6ae3-46aa-a9e1-2e70e760f61c	
	Effectuez le changement de registre suivant	

	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing]	
	State=dword:00010000	
	Redémarrage requis	

Windows 2008R2 (serveur INW)

KB	Lien	Remarques
	Effectuez le changement de registre suivant	
	[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	**Pour installer ce rollup, désinstallez le rollup de juillet KB4025341 et le rollup d'août KB4034664, puis redémarrez le système avant d'appliquer KB4041681** Effectuez le changement de registre suivant – uniquement sur le contrôleur de domaine s'il n'existe pas : [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters] LdapEnforceChannelBinding=DWORD:1

KB4041681 Octobre 2017 Rollup mensuel		**Cette clé de registre est nécessaire sur le contrôleur de domaine** pour démarrer le rollup de juillet KB4025341 (CVE-2017-8563)
	Effectuez le changement de registre suivant	
	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing] **State=dword:00010000**	
	Redémarrage requis	

MLCL V6.9.6 2018 Mises à jour de correctif 3

Les correctifs suivants actualisent le niveau de correctifs du système MLCL et résolvent plusieurs vulnérabilités de sécurité. Les directives suivantes s'appliquent :

1) Les correctifs ci-dessus sont des correctifs requis pour 6.9.6 et doivent être appliqués en premier.
2) Faites attention à la section Notes d'instructions particulières de manipulation.
3) Les correctifs doivent être appliqués dans l'ordre, sauf dans les cas indiqués.
4) Les redémarrages ne sont obligatoires que quand c'est précisé. Si un correctif nécessite un redémarrage à un autre moment, le système peut être redémarré, mais ce n'est pas nécessaire.
5) **Stratégie de mot de passe :** il est possible de modifier la **longueur minimale du mot de passe** et de la définir au-delà de la limite de 14 caractères pour répondre à vos exigences en matière de sécurité.

Suivez ces étapes pour effectuer les changements de registre suivants afin de résoudre les problèmes de vulnérabilité des rollups mensuels de juin et septembre.

Référence : https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8529

Windows 7 (acquisition, examen et examen virtuel) et Windows 2008R2 (serveur INW) :

1. Cliquez sur **Démarrer**, cliquez sur **Exécuter**, tapez **regedt32** ou tapez **regedit**, puis cliquez sur **OK**.
2. Dans l'Éditeur de registre, recherchez le dossier de registre suivant : **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl**
3. Effectuez un clic droit sur **FeatureControl**, sélectionnez **Nouveau**, puis cliquez sur **Clé**.
4. Tapez **FEATURE_ENABLE_PRINT_INFO_DISCLOSURE_FIX**, puis appuyez sur Entrée pour nommer la nouvelle sous-clé.
5. Effectuez un clic droit sur **FEATURE_ENABLE_PRINT_INFO_DISCLOSURE_FIX**, sélectionnez **Nouveau**, puis cliquez sur **Valeur DWORD**.
6. Tapez « iexplore.exe » pour la nouvelle valeur DWORD.
7. Double-cliquez sur la nouvelle valeur DWORD nommée iexplore.exe et définissez le champ de données **Valeur** sur **1**.
8. Cliquez sur **OK** pour fermer.

Windows 2008R2 (serveur INW) :

1. Cliquez sur **Démarrer**, cliquez sur **Exécuter**, tapez **regedt32** ou tapez **regedit**, puis cliquez sur **OK**.
2. Dans l'Éditeur de registre, recherchez le dossier de registre suivant : **HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Internet Explorer\Main\FeatureControl**
3. Effectuez un clic droit sur **FeatureControl**, sélectionnez **Nouveau**, puis cliquez sur **Clé**.
4. Tapez **FEATURE_ENABLE_PRINT_INFO_DISCLOSURE_FIX**, puis appuyez sur Entrée pour nommer la nouvelle sous-clé.
5. Effectuez un clic droit sur **FEATURE_ENABLE_PRINT_INFO_DISCLOSURE_FIX**, sélectionnez **Nouveau**, puis cliquez sur **Valeur DWORD**.
6. Tapez « iexplore.exe » pour la nouvelle valeur DWORD.
7. Double-cliquez sur la nouvelle valeur DWORD nommée iexplore.exe et définissez le champ de données **Valeur** sur **1**.
8. Cliquez sur **OK** pour fermer.

Windows 7 (Acquisition, examen et examen virtuel)		
KB	**Lien**	**Remarques**
	Effectuez le changement de registre suivant	
	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing]	
	State=dword:00023c00	
KB4048957 Rollup mensuel de novembre 2017	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=224b07ab-de98-45f0-8b9c-83551cac66f6	

	Redémarrage requis	
KB4054518 Rollup mensuel de décembre 2017	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=5b48d1cb-83f7-43e1-9308-18872ffe4dce	
	Redémarrage requis	
KB3203468 Juillet 2017 Microsoft Office 2010	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=7a599998-ca41-4840-90ea-8143724e5c6a	
KB3213626 Septembre 2017 Microsoft Office 2010	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=2bb1487f-b287-41a9-b0ec-01b42aa4759e	
KB3128027 Septembre 2017 Microsoft PowerPoint 2010	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=474aa90a-7767-4f4f-b3f5-2ffa12fea4e6	
KB3141537 Septembre 2017 Microsoft Publisher 2010	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=0c646d3e-697d-4463-a6ea-afb3493c5cea	
KB2553338 Octobre 2017 Microsoft Office 2010 SP2	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=14e73852-cbd2-456a-a9a8-7f0c10f1fa40	Un message d'erreur peut apparaître (Impossible d'installer le chemin d'accès de mise à niveau...). Ce message d'erreur peut être ignoré.

KB2837599 Octobre 2017 Microsoft Office 2010 SP2	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=54ccbc02-879e-4aa1-b817-12418ce8dfcd	
KB4011612 Décembre 2017 Microsoft Office 2010 SP2	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=8230d598-8ab1-4efc-89b6-d3507a6dfd20	Un message d'erreur peut apparaître (Impossible d'installer le chemin d'accès de mise à niveau...). Ce message d'erreur peut être ignoré.
KB4011660 Janvier 2018 Microsoft Excel 2010	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=d7594745-04d5-4631-b2d7-289816f4dd43	
KB4011659 Janvier 2018 Microsoft Word 2010	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=0b5a1bf0-3043-47fd-afc3-d2fb55a46a96	
KB4011611 Janvier 2018 Microsoft Office 2010 SP2	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=3b2c376c-ea57-4925-b81d-3b765d456f2b	Extrayez vers un emplacement et exécuter l'extraction à installer. Vérifiez que les mises à jour ont été installées avec succès.
KB4011610 Janvier 2018 Microsoft Office 2010	https://www.microsoft.com/en-us/download/details.aspx?id=56447	
KB4054172 Janvier 2018 .NET Framework	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=537fc3ba-4248-40b8-9498-8a671abebfe9	Installez KB4054172, KB4019990 et KB4054176

KB2719662	Créez les clés de registre suivantes	
	Clé=[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Windows\Sidebar\] Nom de valeur=[TurnOffSidebar] Type=[REG_DWORD] Donnée=[1]	
KB2269637	Créez les clés de registre suivantes	
	Clé=[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\] Nom de valeur=[CWDIllegalInDllSearch] Type=[REG_DWORD] Donnée=[1]	
	Effectuez le changement de registre suivant	
	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing]	
	State=dword:00010000	
	Redémarrage requis	

Windows 2008R2 (serveur INW)

KB	Lien	Remarques
	Effectuez le changement de registre suivant	
	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing]	
	State=dword:00023c00	

KB3177467 ServiceStack	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=f1b99598-a22d-4fbe-9b63-09724833acc3	**Nécessaire pour permettre l'installation du rollup mensuel sans devoir désinstaller le rollup mensuel précédent**
	Redémarrage requis	
KB4048957 Rollup mensuel de novembre 2017	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=435d3006-04ae-4c27-a5f9-3c36f09e58ed	
	Redémarrage requis	
KB4054518 Rollup mensuel de décembre 2017	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=09064e30-6f3e-4c99-8d09-fbc2ba06b436	
	Redémarrage requis	
KB4054172 Janvier 2018 .NET Framework	http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=fdecaf44-50a3-4667-a935-f9e7af0bb317	
KB2269637	Créez les clés de registre suivantes	
	Clé=[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\] Nom de valeur=[CWDIllegalInDllSearch] Type=[REG_DWORD] Donnée=[1]	
	Effectuez le changement de registre suivant	
	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing]	
	State=dword:00010000	
	Redémarrage requis	

Mises à jour de sécurité MLCL v6.9.6 facultatives

Les mises à jour facultatives suivantes peuvent être appliquées pour améliorer le profil de sécurité des systèmes MLCL. Ces mises à jour devraient être évaluées au cas par cas conformément à la stratégie informatique. Les modifications de configuration dans cette section sont compatibles avec la fonctionnalité du produit MLCL mais peuvent avoir un impact informatique sur le site, car les protocoles SSL hérités s'en verront désactivés, ce qui empêchera l'utilisation du bureau à distance et nécessitera une maintenance et une génération de certificat.

	Serveur INW	**Acquisition - Mac-Lab IT/XT/XTi, CardioLab IT/XT/XTi et SpecialsLab**	**Poste de travail client GE de consultation**	**Revue virtuelle**
Correctif	**URL de téléchargement**	**URL de téléchargement**	**URL de téléchargement**	**URL de téléchargement**
MS16-047 **KB3149090** **Remplacé**	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
Plug-in 20007 – Désactiver SSL V2/V3 – KB187498	Voir la section - Comment installer le plug-in 20007 - Désactiver SSL V2/V3 - KB187498	Voir la section - Comment installer le plug-in 20007 - Désactiver SSL V2/V3 - KB187498	Voir la section - Comment installer le plug-in 20007 - Désactiver SSL V2/V3 - KB187498	Voir la section - Comment installer le plug-in 20007 - Désactiver SSL V2/V3 - KB187498
Plug-in 78479 - Poodle	Pas de changement nécessaire. L'étape ci-dessus répare ceci.	Pas de changement nécessaire. L'étape ci-dessus répare ceci.	Pas de changement nécessaire. L'étape ci-dessus répare ceci.	Pas de changement nécessaire. L'étape ci-dessus répare ceci.
Plug-in 35291 – Hachage faible	Voir la section - Comment installer le plug-in 35291 - Hachage faible (Reportez-vous à https://technet.microsoft.com/en-us/library/ms191192(v=sql.105).aspx pour plus d'informations)	Voir la section - Comment installer le plug-in 35291 - Hachage faible (Reportez-vous à https://technet.microsoft.com/en-us/library/ms191192(v=sql.105).aspx pour plus d'informations)	Voir la section - Comment installer le plug-in 35291 - Hachage faible (Reportez-vous à https://technet.microsoft.com/en-us/library/ms191192(v=sql.105).aspx pour plus d'informations)	Voir la section - Comment installer le plug-in 35291 - Hachage faible (Reportez-vous à https://technet.microsoft.com/en-us/library/ms191192(v=sql.105).aspx pour plus d'informations)
Plug-in 45411	Pas de changement nécessaire. L'étape ci-dessus répare ceci.	Pas de changement nécessaire. L'étape ci-dessus répare ceci.	Pas de changement nécessaire. L'étape ci-dessus répare ceci.	Pas de changement nécessaire. L'étape ci-dessus répare ceci.

	Serveur INW	Acquisition - Mac-Lab IT/XT/XTi, CardioLab IT/XT/XTi et SpecialsLab	Poste de travail client GE de consultation	Revue virtuelle
Plug-in 65821 - Suites de chiffrement SSL RC4 prises en charge (bar Mitzvah)	Voir la section - Comment installer le plug-in 65821 - Suites de chiffrement SSL RC4 prises en charge (bar Mitzvah)	Voir la section - Comment installer le plug-in 65821 - Suites de chiffrement SSL RC4 prises en charge (bar Mitzvah)	Voir la section - Comment installer le plug-in 65821 - Suites de chiffrement SSL RC4 prises en charge (bar Mitzvah)	Voir la section - Comment installer le plug-in 65821 - Suites de chiffrement SSL RC4 prises en charge (bar Mitzvah)
Plug-in 63155 - Énumération de chemin d'accès du service Microsoft Windows sans guillemets	Voir la section - Comment supprimer une vulnérabilité pour le plug-in 63155 - Énumération de chemin d'accès du service Microsoft Windows sans guillemets	Voir la section - Comment supprimer une vulnérabilité pour le plug-in 63155 - Énumération de chemin d'accès du service Microsoft Windows sans guillemets	Voir la section - Comment supprimer une vulnérabilité pour le plug-in 63155 - Énumération de chemin d'accès du service Microsoft Windows sans guillemets	Voir la section - Comment supprimer une vulnérabilité pour le plug-in 63155 - Énumération de chemin d'accès du service Microsoft Windows sans guillemets
Plug-in 59915 - Des vulnérabilités dans les gadgets pourraient permettre l'exécution de code à distance	S/O	Veuillez suivre la section intitulée **"Disable the Sidebar in the system Registry"** (Désactiver la barre latérale dans le registre système) dans l'article suivant : https://technet.microsoft.com/library/security/2719662	Veuillez suivre la section intitulée **"Disable the Sidebar in the system Registry"** (Désactiver la barre latérale dans le registre système) dans l'article suivant : https://technet.microsoft.com/library/security/2719662	Veuillez suivre la section intitulée **"Disable the Sidebar in the system Registry"** (Désactiver la barre latérale dans le registre système) dans l'article suivant : https://technet.microsoft.com/library/security/2719662
Désactivation du protocole SMB1	Consultez la section Comment désactiver le protocole SMB1	Consultez la section Comment désactiver le protocole SMB1	Consultez la section Comment désactiver le protocole SMB1	Consultez la section Comment désactiver le protocole SMB1

Stratégie de mot de passe

Stratégie de mot de passe : Il est possible de modifier la longueur minimale du mot de passe et de la définir au-delà de la limite de 14 caractères pour répondre à vos exigences en matière de sécurité. Reportez-vous à la section **Mot de passe** du Guide de sécurité pour plus de détails sur la modification des mots de passe.

Coordonnées

Si vous avez des questions supplémentaires, veuillez contacter notre assistance technique.