Correctif logiciel LRM 1.0

illumina®

Guide d'utilisation

Introduction

Illumina® a pris connaissance d'une vulnérabilité de sécurité présente dans le logiciel Local Run Manager et fourni un correctif afin de vous protéger contre toute exploitation à distance de cette vulnérabilité.

Local Run Manager est une application logicielle autonome qui fait partie de la configuration par défaut des systèmes suivants :

- MiSeq
- MiSeqDx*
- NextSeq 500
- NextSeq 550
- NextSeq 550Dx*
- MiniSeq
- iSeq

*Pour diagnostic in vitro.

Ce guide s'applique aux instruments Illumina énumérés ci-dessus ainsi qu'aux ordinateurs hors-instrument sur lesquels la version autonome de Local Run Manager est installée.

La vulnérabilité est une exécution de commande à distance non authentifiée (RCE) avec un score CVSS non atténué de 10.0 Critique, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H`.

Les méthodes d'atténuation suivantes sont requises sur les instruments énumérés ci-dessus afin de se protéger contre la possibilité qu'une personne non autorisée accède à un ou plusieurs instruments et exécute une attaque à distance.

Si, pour une raison quelconque, le programme d'installation ne peut pas être exécuté, consultez la section sur les méthodes d'atténuation supplémentaires à la fin de ce document, ou communiquez avec techsupport@illumina.com pour bénéficier d'une assistance supplémentaire.

Consultez la rubrique Obtenir la mise à jour de Local Run Manager pour découvrir les options permettant de télécharger ou de demander une copie du correctif.

- **Version du correctif v1.0.0** : met à jour la configuration web de Local Run Manager et désactive l'accès distant à Internet Information Services (IIS).

Obtention du correctif de sécurité de Local Run Manager

Il existe quatre (4) manières d'obtenir le correctif de sécurité Local Run Manager.

Option 1 : téléchargez-le directement sur votre instrument

Le moyen le plus rapide d'obtenir la mise à jour de sécurité de Local Run Manager est de la télécharger directement du site web d'hébergement vers l'instrument.

1. Téléchargez le programme d'installation du correctif à partir du lien fourni par un e-mail sécurisé à votre instrument.
2. Transférez le fichier dans le dossier `C:\Illumina` sur l'instrument.
3. Suivez les instructions de la section *Installation du correctif de sécurité de Local Run Manager*, page 4.

Option 2 : téléchargez le programme d'installation du correctif sur l'ordinateur et transférez-le sur l'instrument via une clé USB ou un dossier partagé.

Si vous ne pouvez pas télécharger le correctif de sécurité sur l'instrument, nous vous recommandons de le télécharger sur un autre ordinateur puis de le transférer sur l'instrument.

Vérifiez l'intégrité de la clé USB avec vos représentants de sécurité avant toute utilisation. (Recommandé)

1. Téléchargez le programme d'installation du correctif à partir du lien fourni dans le courriel sécurisé sur votre ordinateur ou votre portable.
2. Copiez le programme d'installation du correctif téléchargé sur la clé USB ou le dossier partagé de l'ordinateur.
3. Si vous utilisez la clé USB, branchez-la sur l'instrument.
4. Copiez le programme d'installation du correctif depuis la clé USB ou le dossier partagé vers le dossier `C:\Illumina` de l'instrument.
5. Suivez les instructions de la section *Installation du correctif de sécurité de Local Run Manager*, page 4.

Option 3 : demandez de l'aide à l'assistance technique

Un représentant de l'assistance technique d'Illumina vous guidera dans le processus de correction en utilisant l'une des méthodes suivantes :

- Connexion à distance à l'assistance technique

  Un représentant de l'assistance technique se connectera à distance à l'analyseur et installera le correctif au nom du client.

  Le système doit être accessible à distance. Si vous avez des questions, posez-les à votre représentant informatique local pour obtenir de l'aide.

- Instructions guidées
  Un représentant de l'assistance technique vous donnera des instruction guidées par téléphone. Veuillez communiquer avec votre représentant local de l'assistance technique pour obtenir de l'aide.

Option 4 : commandez une clé préconfigurée chez Illumina

Une clé USB protégée en écriture peut être commandée gratuitement par le client. Pour commander la clé avec un correctif déjà installé, veuillez communiquez avec l'assistance technique à l'adresse techsupport@illumina.com.

Il pourrait y avoir des retards d'expéditions ou de stocks pouvant affecter la rapidité de la livraison. Pour protéger les systèmes de manière plus immédiate, il est vivement recommandé de les protéger par la méthode qui permettra de résoudre le problème de la manière la plus efficace.

Exécuter le correctif de sécurité Local Run Manager v.1.0.

Une fois exécuté, le MSI (Microsoft Installer) d'Illumina mettra à jour la configuration du serveur web de Local Run Manager afin d'empêcher l'exécution de tout contenu téléchargé par l'utilisateur et de bloquer tout accès à distance à l'interface web de Local Run Manager à partir des connexions du réseau local.

Les utilisateurs ne pourront plus utiliser l'interface web de Local Run Manager pour avoir accès à distance aux instruments et ce flux de travail cessera de fonctionner après l'installation de ce correctif. Illumina a l'intention de restaurer ultérieurement cette fonctionnalité avec le correctif logiciel permanent pour ce problème. Si cela entraîne une interruption des flux de travail définis, veuillez communiquer avec techsupport@illumina.com pour obtenir une assistance supplémentaire.

Le programme d'installation MSI prend en charge toutes les versions de Local Run Manager et détecte automatiquement le correctif approprié en fonction de la version de Local Run Manager installée sur l'instrument/l'ordinateur.

Ce programme d'installation MSI créera également un fichier d'audit montrant que cette méthode d'atténuation a été mise en œuvre, ainsi qu'un horodatage pour refléter l'installation correcte.

Exécution du programme d'installation MSI – lors de la première exécution du programme d'installation MSI, ce dernier applique le correctif au système et crée un fichier d'audit indiquant l'heure de fin du travail.

En exécutant à nouveau le programme d'installation MSI, une option **Repair (Réparation)** apparaît. Cette option permet à l'utilisateur de réappliquer ou d'annuler le correctif. Remarque : l'annulation du correctif rendra une configuration de l'instrument vulnérable.

Installation du correctif de sécurité de Local Run Manager

Pour installer le correctif :

1. Connectez-vous au système via un compte administrateur (par exemple sbsadmin).

   Illumina recommande d'appliquer le correctif lorsque l'instrument n'est pas en cours d'utilisation. Si l'instrument est en train d'exécuter un cycle, le correctif doit être appliqué immédiatement après la fin du cycle.

2. Recherchez le correctif qui a été téléchargé sur le système.
3. Déplacez le programme d'installation du correctif vers le dossier `C:\Illumina` (exempt de la politique de restriction des logiciels).
4. Double-cliquez sur l'icône du programme d'installation pour démarrer l'interface.
5. Lors du chargement de l'application, sélectionnez **Next (Suivant)** pour démarrer l'installation du correctif.
6. Sur l'écran Installation completion (Fin de l'installation), sélectionnez **Finish (Terminer)**.

Si une vérification du rapport de l'installation est nécessaire, veuillez consulter la section *Vérification*, page 5.

Il est nécessaire de redémarrer à la fin de l'installation

Réparation

En cas d'erreur, le client peut procéder à la réparation de l'installation en suivant les instructions ci-dessous :

1. Connectez-vous au système via un compte administrateur (par exemple sbsadmin).
2. Recherchez le correctif qui a été téléchargé sur le système.
3. Déplacez le programme d'installation du correctif vers le dossier `C:\Illumina` (exempt de la politique de restriction des logiciels).
4. Double-cliquez sur l'icône du programme d'installation pour démarrer l'interface.
5. Le programme d'installation détectera automatiquement si l'outil de configuration a été exécuté auparavant et représentera de nouvelles options :
   a. Change (Modifier) : Grisé et indisponible
   b. Repair (Réparer) : Répare les erreurs et propose des options de reconfiguration.
   c. Remove (Supprimer) : Désinstalle le correctif et le restaure à sa configuration par défaut (consultez *Désinstallation*, page 5)
6. Sur l'écran Installation completion (Fin de l'installation), sélectionnez **Finish (Terminer)**.

Si une vérification du rapport de l'installation est nécessaire, veuillez consulter la section *Vérification*, page 5.

Il est nécessaire de redémarrer à la fin de l'installation

Désinstallation

La désinstallation du correctif annule les modifications apportées au fichier de configuration de l'hôte de l'application.

1. Connectez-vous au système via un compte administrateur (par exemple sbsadmin).
2. Recherchez le correctif qui a été téléchargé sur le système.
3. Déplacez le programme d'installation du correctif vers le dossier `C:\Illumina` (exempt de la politique de restriction des logiciels).
4. Double-cliquez sur l'icône du programme d'installation pour démarrer l'interface.
5. Sélectionnez **Remove (Supprimer)** pour désinstaller le correctif et rétablir toutes les valeurs par défaut.
6. Sélectionnez **Remove (Supprimer)** pour vérifier l'option permettant de désinstaller le correctif et de rétablir toutes les valeurs par défaut.

Ce paramètre rendra le système non sécurisé et vulnérable aux attaques. Il est vivement recommandé de prendre en compte les impacts techniques à l'origine de l'option de suppression du correctif avant de choisir de le désinstaller.

7. Sur l'écran Installation completion (Fin de l'installation), sélectionnez **Finish (Terminer)**.

Si une vérification du rapport de l'installation est nécessaire, veuillez consulter la section *Vérification*, page 5.

Un redémarrage à la fin de l'installation est recommandé.

Vérification

S'il est nécessaire de vérifier l'installation, un fichier de vérification aura été généré et comprendra un horodatage, la version de Local Run Manager installée et d'autres valeurs de vérification clés. Pour obtenir ce fichier, veuillez communiquer avec techsupport@illumina.com.

Recommandations supplémentaires en matière d'atténuation et de sécurité

La sécurité du déploiement des instruments RUO et des dispositifs médicaux Dx dépend des couches de sécurité. Illumina recommande vivement le déploiement des instruments et des dispositifs dans le plus petit sous-réseau ou contexte de sécurité du réseau, avec des dispositifs fiables. Il est vivement recommandé d'utiliser des pares-feux et d'autres politiques de réseau pour limiter les autres accès entrants et sortants.

Nous recommandons également les mesures suivantes :

- Activez le protocole TLS (Sécurité de la couche de transport) pour garantir que toutes les communications hors instrument sont cryptées.
  - Pour activer le protocole TLS (Sécurité de la couche de transport), veuillez consulter le guide du logiciel Local Run Manager.

Autres options

Si, pour une raison quelconque, l'exécution du correctif n'est pas possible, les méthodes d'atténuation manuelles suivantes permettront de réduire le risque :

- Désactivez l'accès à distance au logiciel Local Run Manager en y ajoutant des règles de pare-feu Windows pour bloquer les connexions entrantes des ports 80 et 443.
  Le programme d'installation MSI bloque automatiquement les connexions entrantes à distance dans la configuration du serveur web de Local Run Manager. Une autre méthode d'atténuation manuelle qui permet d'obtenir le même résultat consiste à configurer le pare-feu Windows de manière à bloquer les connexions entrantes aux connexions `HTTP (TCP:80)` et `HTTPS (TLS, TCP:443)`.
  Une fois installé, Local Run Manager ne sera accessible que sur l'ordinateur sur lequel il est installé ; il ne sera plus accessible à partir d'autres ordinateurs connectés au même réseau.

> Si le flux de travail de l'utilisateur nécessite un accès à distance à Local Run Manager, cette fonctionnalité ne fonctionnera plus.

- Réduisez le nombre d'autres périphériques réseau.
  Configurer le réseau de manière à réduire le nombre d'autres périphériques réseau pouvant communiquer avec l'instrument affecté réduira le risque d'exploitation. Moins il y a de connexions au système, moins il y a de possibilités d'accès.
  L'exécution de cette tâche peut nécessiter une consultation auprès de votre service local de sécurité de l'information ou des ressources informatiques.
- Déconnectez l'instrument du réseau.
  En l'absence de toute autre option, la dernière méthode d'atténuation consiste à déconnecter complètement l'instrument du réseau. Cela désactivera l'accès aux services Illumina Cloud/SaaS tels que Proactive et BaseSpace® Sequence Hub, ainsi qu'aux flux de travail de déchargement de données génomiques types.
  L'exécution de cette tâche peut nécessiter une consultation auprès de votre service local de sécurité de l'information ou des ressources informatiques.

Recherche d’un accès non autorisé potentiel

Les étapes suivantes peuvent aider l’opérateur de l’instrument à déterminer si un utilisateur non autorisé a accédé au système :

1. Examinez les journaux IIS conservés dans `C:\inetpub\logs\LogFiles\W3SVC1` pour rechercher d’éventuels appels anormaux.
   - Les appels normaux émis vers le serveur web Local Run Manager se présentent comme suit :

     ```
     GET http /normalresource.extension?normal-URI-decoration
     ```

   - Les appels anormaux émis vers le serveur web Local Run Manager peuvent, par exemple, se présenter comme suit :

     ```
     POST http /hackertool.asp
     ```

2. Examinez le journal IIS pour rechercher d’éventuels chargements POST de contenu autre que des fichiers de manifeste. Par exemple, les appels suivants peuvent indiquer une activité suspecte :

   ```
   wscript
   shell
   wscript.network
   scripting.filesystemObject
   ```

3. Si une application anti-virus ou anti-logiciels malveillants est installée, consultez ses journaux pour rechercher d’éventuels signes de comportement anormal.
4. Examinez les journaux Windows pour rechercher d’éventuels messages anormaux.
   Si un acteur malveillant est parvenu à obtenir un accès avec des droits d’administration, il aura eu la capacité de modifier ou de supprimer tous les journaux et événements locaux des instruments.

Recherchez les points de terminaison auxquels le système a tenté d’accéder. Pour connaître la liste des connexions sortantes normales, consultez Contrôler le pare-feu informatique.

Contactez l’assistance technique d’Illumina pour obtenir de l’aide en cas de besoin.

Historique de révision

Document	Date	Description de la modification
Document # 200017330 v02	Avril 2022	Ajout d’une recommandation invitant à appliquer le correctif lorsque l’instrument n’est pas utilisé. Ajout d’une instruction indiquant que le redémarrage de l’instrument est nécessaire après l’installation du patch. Correction de la description de l’historique de version pour la version v01.
Document # 200017330 v01	Avril 2022	Modification du titre du document, remplacé par Guide d’utilisation du correctif logiciel LRM 1.0 Suppression de toute mention de v1.0.1. Ajout d’une section couvrant la recherche d’un accès non autorisé potentiel.
Document # 200017330 v00	Mars 2022	Publication initiale.