Correctif logiciel LRM 1.0

illumina[MD]

Guide d'instructions

Introduction

Illumina[MD] a appris que le logiciel Local Run Manager présentait une vulnérabilité de sécurité et a développé un correctif logiciel pour vous protéger contre l'exploitation à distance de cette vulnérabilité.

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

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

* Destiné au diagnostic in vitro uniquement.

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

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

Les étapes d'atténuation suivantes sont nécessaires sur les instruments énumérés ci-dessus pour se protéger contre le risque qu'un utilisateur non autorisé accède à un ou plusieurs instruments et exécute une attaque sur les accès à distance.

Si pour une raison quelconque, le programme d'installation ne peut pas être exécuté, consultez la section relative aux autres méthodes d'atténuation à la fin de ce document ou communiquez avec techsupport@illumina.com pour obtenir de l'aide.

Consultez la section Obtenir la mise à jour de Local Run Manager pour savoir comment télécharger ou demander une copie du correctif.

- **Correctif v1.0.0** : il mettra à jour la configuration Web de Local Run Manager et désactivera l'accès aux services Internet (IIS) à distance.

Obtenir le correctif de sécurité de Local Run Manager

Il y a quatre (4) options pour obtenir le correctif de sécurité de Local Run Manager.

Option 1 : Le télécharger 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 sur l'instrument à partir du site Web d'hébergement.

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

Option 2 : Télécharger le programme d'installation du correctif sur l'ordinateur et le transférer vers l'instrument en utilisant la clé USB/le dossier partagé

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

Vérifiez l'intégrité de la clé USB auprès des responsables de la sécurité avant toute utilisation. (Recommandé)

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

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

Un représentant de l'assistance technique d'Illumina vous guidera tout au long du processus de la mise à jour corrective en utilisant l'une des méthodes suivantes :

- Connexion à distance à l'assistance technique

  Un représentant de l'assistance technique accèdera à distance à l'analyseur et installera le correctif pour le compte du client.

  Le système doit être accessible à distance. Si vous avez des questions, posez-les au représentant des TI de votre région pour qu'il vous aide.

- Instructions guidées
  Un représentant de l’assistance technique donnera des instructions guidées par téléphone. Veuillez communiquer avec le représentant de l’assistance technique de votre région pour obtenir de l’aide.

Option 4 : Commander une clé préconfigurée auprès d’Illumina

Le client peut commander gratuitement une clé USB protégée en écriture. Pour commander la clé avec le correctif, veuillez communiquer avec l’assistance technique en envoyant un courriel à l’adresse techsupport@illumina.com.

Il pourrait y avoir des retards d’expédition ou de stock pouvant influencer la rapidité de la livraison. Pour protéger les systèmes sans délai, il est vivement recommandé de protéger les systèmes en utilisant la méthode la plus efficace.

Exécuter le programme d’installation pour appliquer le correctif de sécurité v.1.0 de Local Run Manager

Lorsqu’il est exécuté, le programme d’installation MSI (Microsoft Installer) d’Illumina mettra à jour la configuration du serveur Web Local Run Manager pour éviter l’exécution de tout contenu utilisateur téléversé et bloquer toute tentative d’accès à distance à l’interface Web de Local Run Manager à partir des connexions réseau LAN.

Les utilisateurs ne pourront plus utiliser l’interface Web de Local Run Manager pour accéder à distance aux instruments après l’installation de ce correctif. Illumina a l’intention de restaurer ultérieurement cette fonction 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 de l’aide.

Le programme d’installation MSI prend en charge toutes les versions de Local Run Manager et déterminera automatiquement le correctif approprié selon 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 une installation correcte.

Exécution du programme d’installation MSI : lors de la première exécution du programme d’installation MSI, ce dernier applique le correctif sur le système et crée un fichier d’audit avec l’heure de fin du travail.

Une nouvelle option **Repair** (Réparer) apparaît lorsque le programme d’installation MSI est de nouveau exécuté. Grâce à cette option, l’utilisateur peut réappliquer ou annuler le correctif. Remarque : l’annulation du correctif rendra la configuration de l’instrument vulnérable.

Appliquer le 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 marche. Si l'instrument exécute une analyse, le correctif doit être appliqué juste après qu'elle ait fini.

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 stratégie de restriction logicielle).
4. Double-cliquez sur l'icône du programme d'installation pour lancer l'interface.
5. Lors du chargement de l'application, sélectionnez **Next** (Suivant) pour commencer l'installation du correctif.
6. À l'écran Installation Completion (Fin de l'installation), sélectionnez **Finish** (Terminer).

Si une vérification du rapport d'installation est requise, veuillez vous reporter à la section *Vérification*, page 5.

Il est nécessaire de procéder à un redémarrage à la fin de l'installation.

Réparer

En cas d'erreur, le client peut exécuter la réparation de l'installation en suivant les consignes 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 stratégie de restriction logicielle).
4. Double-cliquez sur l'icône du programme d'installation pour lancer l'interface.
5. Le programme d'installation détectera automatiquement si l'outil de configuration a été exécuté au préalable et présentera de nouvelles options :
   a. Change (Modifier) : grisée et non disponible
   b. Repair (Réparer) : répare les erreurs et propose des options pour la reconfiguration.
   c. Remove (Supprimer) : désinstalle le correctif et restaure la configuration par défaut (consultez la section *Désinstallation*, page 5).
6. À l'écran Installation Completion (Fin de l'installation), sélectionnez **Finish** (Terminer).

Si une vérification du rapport d'installation est requise, veuillez vous reporter à la section *Vérification*, page 5.

Il est nécessaire de procéder à un redémarrage à la fin de l'installation.

Désinstallation

La désinstallation du correctif rétablit les modifications apportées au fichier de configuration 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 stratégie de restriction logicielle).
4. Double-cliquez sur l'icône du programme d'installation pour lancer l'interface.
5. Sélectionnez **Remove** (Supprimer) pour désinstaller le correctif et rétablir tous les paramètres par défaut.
6. Sélectionnez **Remove** (Supprimer) pour vérifier l'option de désinstallation du correctif et rétablir tous les paramètres par défaut.

Ce paramètre rendra le système vulnérable et l'exposera au risque d'attaques. Il est fortement recommandé de tenter de résoudre les problèmes techniques qui appellent à la suppression du correctif avant de choisir de le désinstaller.

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

Si une vérification du rapport d'installation est requise, veuillez vous reporter à la section *Vérification*, page 5.

Il est recommandé de procéder à un redémarrage à la fin de l'installation.

Vérification

Si nécessaire, vérifiez l'installation en utilisant le fichier de vérification généré comportant un horodatage, la version du logiciel Local Run Manager installée et d'autres valeurs de vérification clés. Pour obtenir ce fichier, veuillez envoyer un courriel à l'adresse techsupport@illumina.com.

Recommandations de sécurité et mesures d'atténuation supplémentaires

Le déploiement sécurisé des instruments en mode recherche (RUO) et des dispositifs médicaux de diagnostic dépend des couches de sécurité. Illumina recommande vivement de déployer les instruments et les dispositifs dans le plus petit sous-réseau ou contexte de sécurité, avec des dispositifs de confiance. Il est vivement conseillé d'utiliser des pare-feu et d'autres stratégies réseau pour limiter l'accès entrant et sortant.

Nous recommandons également ce qui suit :

- Activez le protocole de sécurité de la couche de transport (TLS) pour vous assurer que toutes les communications externes sont chiffrées.
  - Pour activer le protocole TLS, veuillez consulter le guide du logiciel Local Run Manager.

Autres options

Si pour une raison quelconque, l'exécution du correctif ne peut pas être envisagée, les méthodes d'atténuation manuelles indiquées ci-après permettront de réduire les risques :

- Désactivez l'accès à distance à Local Run Manager en ajoutant des règles de pare-feu Windows pour bloquer les connexions entrantes aux ports 80 et 443.
  Le programme d'installation MSI bloquera automatiquement les connexions à distance entrantes 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 mettre en œuvre une configuration de pare-feu Windows pour bloquer les connexions entrantes aux connexions `HTTP (TCP:80)` et `HTTPS (TLS, TCP:443)`.
  Après la mise en œuvre, Local Run Manager n'est accessible que sur l'ordinateur sur lequel il est installé; il ne sera plus accessible à partir des ordinateurs connectés au même réseau.

> Si le flux de travail de l'utilisateur nécessite d'accéder à distance à Local Run Manager, cette fonction 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 concerné minimisera le risque pour l'exploitation. Moins il y a de connexions au système, plus l'accès est limité.
  Vous devrez peut-être consulter le service local chargé de la sécurité de l'information ou les ressources des technologies de l'information pour l'exécution.
- Retirez l'instrument du réseau.
  Si aucune autre option n'est possible, la dernière méthode d'atténuation consiste à retirer complètement l'instrument du réseau. Veuillez noter que cela désactivera l'accès aux services infonuagiques/SaaS d'Illumina tels que Proactive et BaseSpaceMD Sequence Hub, ainsi qu'aux flux de travail de déchargement des données génomiques types.
  Vous devrez peut-être consulter le service local chargé de la sécurité de l'information ou les ressources des technologies de l'information pour l'exécution.

Investigation des accès non autorisés potentiels

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

1. Examinez les journaux IIS enregistrés sous `C:\inetpub\logs\LogFiles\W3SVC1` pour identifier les appels anormaux.
   - Les appels normaux vers le serveur Web Local Run Manager apparaissent de la manière suivante :

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

   - Des appels anormaux vers le serveur Web Local Run Manager peuvent apparaître de la manière suivante :

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

2. Examinez le journal IIS pour voir si un contenu POST autre que celui des fichiers de manifeste a été téléversé. Par exemple, les appels suivants pourraient indiquer une activité suspecte :

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

3. Si une application anti-virus/anti-programme malveillant est installée, vérifiez les journaux du logiciel pour surveiller les signes d'un comportement inhabituel.
4. Examinez les journaux Windows pour détecter la présence de messages d'erreur anormaux.
   Si une personne malveillante se connecte avec des droits d'administrateur, elle pourra modifier ou supprimer tous les événements et journaux locaux de l'instrument.

Surveillez les points de terminaison pour identifier les tentatives d'accès au système. Pour connaître la liste des connexions sortantes prévues, reportez-vous au Pare-feu de l'ordinateur de commande.

Communiquez avec l'assistance technique d'Illumina pour obtenir du soutien.

Historique des révisions

Document	Date	Description des modifications
Document n° 200017330 v02	Avril 2022	Ajout d’une recommandation pour appliquer le correctif lorsque l’instrument n’est pas en marche. Ajout de la consigne de redémarrer l’instrument après l’installation du correctif. Correction de la description de l’historique de révision pour la v01.
Document n° 200017330 v01	Avril 2022	Titre du document remplacé par Guide d’instructions du correctif logiciel LRM 1.0. Retrait de toute mention de la v1.0.1. Ajout de la section relative à l’investigation des accès non autorisés potentiels.
Document n° 200017330 v00	Mars 2022	Publication originale.