illumina®

LRM Software Patch 1.0

دليل الإرشادات

المقدمة

لقد أصبحت Illumina® على دراية بالثغرة الأمنية الموجودة في برنامج مدير التشغيل المحلي وقدمت تصحيحًا للبرنامج للحماية من الاستغلال عن بُعد لهذه الثغرة الأمنية.

برنامج مدير التشغيل المحلي عبارة عن تطبيق برنامج مستقل بذاته وجزء من التكوين الافتراضي للأنظمة التالية:

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

"لأغراض الاستخدام في التشخيص المختبري فقط"

ينطبق هذا الدليل على أجهزة Illumina المذكورة أعلاه وأيضًا على أجهزة الكمبيوتر غير المستخدمة والتي تم تثبيت الإصدار المستقل من برنامج مدير التشغيل المحلي عليها.

تُعد الثغرة الأمنية عبارة عن تنفيذ لأوامر غير مُصرح بها عن بُعد (RCE) على أن تكون درجة نظام تسجيل نقاط الضعف المشترك (CVSS) التامّة من 10.0، أي درجة حرجة، `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H`.

خطوات التخفيف التالية مطلوبة على الأدوات المذكورة أعلاه للحماية من إمكانية وصول مستخدم غير مصرح له إلى أداة أو أكثر وتنفيذ هجوم وصول عن بعد.

وفي حال تعذّر تشغيل المُثبّت لسببٍ ما، راجع قسم إجراءات التخفيف من المخاطر الإضافية الواردة في نهاية هذا المستند، أو تواصل مع techsupport@illumina.com للحصول على المزيد من المساعدة.

راجع الحصول على تحديث برنامج مدير التشغيل المحلي للاطلاع على خيارات تتعلّق بكيفية تنزيل نسخة من التصحيح أو طلبها.

- **التصحيح إصدار 1.0.0-** سيعمل على تحديث تكوين الويب لبرنامج مدير التشغيل المحلي وتعطيل الوصول عن بُعد إلى خدمات معلومات الإنترنت (IIS).

الحصول على تصحيح الأمان الخاص ببرنامج مدير التشغيل المحلي

هناك أربعة (4) خيارات للحصول على تصحيح أمان مدير التشغيل المحلي.

الخيار **1** —التنزيل إلى جهازك مباشرةً

تتمثل الطريقة الأسرع للحصول على تحديث الأمان لبرنامج مدير التشغيل المحلي في تنزيله مباشرةً من موقع المضيف الإلكتروني إلى الجهاز.

1. نزل مُثبّت التصحيح من الرابط المتوفر عبر البريد الإلكتروني الآمن إلى جهازك.
2. انقل الملف إلى مجلد `C:\Illumina` الموجود على الجهاز.
3. اتبع التعليمات الواردة في *تطبيق تصحيح الأمان الخاص ببرنامج مدير التشغيل المحلي* على الصفحة 3.

الخيار **2** — تنزيل أداة تثبيت التصحيح إلى جهاز الكمبيوتر ونقله إلى الأداة عبر محرك أقراص **USB/** مجلد مشترك

إذا لم تتمكن من تنزيل تصحيح الأمان للأداة، نوصي بتنزيله إلى جهاز كمبيوتر منفصل ثم نقله إلى الجهاز.

تحقق من سلامة محرك أقراص USB مع ممثلي الأمان لديك قبل الاستخدام. (موصى به)

1. قم بتنزيل مُثبّت التصحيح من الرابط المتوفر عبر البريد الإلكتروني الآمن إلى الكمبيوتر أو الكمبيوتر المحمول الخاص بك.
2. انسخ مُثبّت التصحيح الذي تم تنزيله على محرك أقراص USB أو المجلد المشترك من جهاز الكمبيوتر.
3. بالنسبة لمحرك أقراص USB، قم بتوصيل محرك الأقراص بالجهاز.
4. انسخ مُثبّت التصحيح من محرك أقراص USB أو المجلد المشترك إلى مجلد `C:\Illumina` المتوفر على الجهاز.
5. اتبع التعليمات الواردة في *تطبيق تصحيح الأمان الخاص ببرنامج مدير التشغيل المحلي* على الصفحة 3.

الخيار **3** —طلب الدعم الفني

سيُرشدك أحد ممثلي الدعم الفني لدى Illumina خلال عملية التصحيح باستخدام إحدى الطرق التالية:

- تسجيل دخول الدعم الفني عن بُعد

  سيقوم ممثل الدعم الفني بالوصول إلى أداة التحليل عن بعد وتثبيت التصحيح نيابة عن العميل.

  يلزم الوصول إلى النظام عن بُعد. إذا كانت لديك أي أسئلة، فاطلب المساعدة من مُمثل تكنولوجيا المعلومات المحلي لديك.

- الإر شادات التوجيهية

  سيُقدم ممثل الدعم الفني إر شادات توجيهية عبر الهاتف. يُرجى التواصل مع ممثل الدعم الفني المحلي لديك للحصول على المساعدة.

الخيار **4** — طلب محرك أقراص مُكوّن مسبقًا من **Illumina**

يُمكن أن يطلب العميل محركات أقراص USB محمية ضد الكتابة دون أي تكلفة. لطلب محرك الأقراص المُثبّت عليه التصحيح، يُرجى التواصل مع techsupport@illumina.com.

قد تحدث تأخيرات بسبب عمليات الشحن أو جرد المخزون ما قد يؤثر على الجداول الزمنية للتسليم. ولحماية الأنظمة بشكل فوري، يُوصى بشدة بحماية الأنظمة بالطريقة التي ستوفر المسار الأكثر فعالية للحل.

تطبيق تصحيح الأمان الخاص ببرنامج تشغيل مدير التشغيل المحلي إصدار v.1.0

سيعمل MSI(Microsoft Installer) لدى Illumina، عند تطبيقه، على إصلاح تكوين خادم ويب برنامج مدير التشغيل المحلي لمنع تنفيذ أي محتوى تم تحميله للمستخدم وحظر جميع عمليات الوصول عن بُعد إلى واجهة ويب برنامج مدير التشغيل المحلي من اتصالات شبكة LAN.

وبالنسبة لهؤلاء المستخدمين ممّن يستخدمون واجهة ويب برنامج مدير التشغيل المحلي للوصول إلى الأجهزة عن بُعد، سيتوقف سير العمل هذا عن العمل بعد تثبيت هذا التصحيح. تهدف Illumina إلى استعادة هذه الوظيفة من خلال إصلاح البرنامج فيما يتعلّق بهذه المشكلة بصورة دائمة لاحقًا. إذا تسببت هذه المشكلة في انقطاع لعمليات سير العمل التي أُنشئت، فيُرجى التواصل مع techsupport@illumina.com للحصول على المزيد من المساعدة.

يُعدّ مُثبت MSI قابلًا للتطبيق على جميع إصدارات برنامج مدير التشغيل المحلي و سيُحدد تلقائيًا عملية الإصلاح الصحيحة بناءً على إصدار برنامج مدير التشغيل المحلي المُثبّت على الجهاز/الكمبيوتر.

كما سيعمل مُثبت MSI هذا كذلك على إنشاء ملف تدقيق يعرض أنه جرى تنفيذ إجراء التخفيف من المخاطر هذا إلى جانب طابع زمني ليعكس عملية تثبيت صحيحة.

تشغيل مُثبت MSI – عند تشغيل مُثبت MSI للمرة الأولى، سيعمل المُثبت على تصحيح النظام وإنشاء ملف تدقيق مُدرج به وقت الإكمال.

سيعرض مُثبت MSI، عند تشغيله مرة أخرى، الخيار **Repair** (إصلاح)، ويُمنح المستخدم هذا الخيار لإعادة تطبيق عملية التصحيح أو التراجع عنها. ملاحظة: سيتسبب التراجع عن عملية التصحيح في تكوين غير آمن للجهاز.

تطبيق تصحيح الأمان الخاص ببرنامج مدير التشغيل المحلي

لتثبيت التصحيح:

1. سجّل الدخول إلى النظام عبر حساب مسؤول (على سبيل المثال sbsadmin).

توصي شركة Illumina بتطبيق التصحيح عندما لا تكون الأداة قيد التشغيل. إذا كانت الأداة تقوم بتنفيذ عملية تشغيل، فيجب تطبيق التصحيح على الفور بعد اكتمال التشغيل.

2. حدد مكان التصحيح الذي تم تنزيله على النظام.
3. انقل مُثبّت التصحيح إلى مجلد `C:\Illumina` (مُعفى من نهج تقييد البرامج).
4. انقر نقرًا مزدوجًا على أيقونة المُثبّت لتشغيل الواجهة.
5. عند تحميل التطبيق، حدد **Next** (التالي) لبدء تثبيت التصحيح.
6. في شاشة Installation Completion (إكمال عملية التثبيت)، حدد **Finish** (إنهاء).

إذا كان يلزم التحقق من تقرير التثبيت، فيُرجى مراجعة قسم *التحقق* على الصفحة 4.

يوصى بإعادة التشغيل في نهاية التثبيت.

الإصلاح

في حال وقوع خطأ ما، يُمكن أن يُجري العميل إصلاحًا لعملية التثبيت من خلال اتباع الإر شادات التالية:

1. سجّل الدخول إلى النظام عبر حساب مسؤول (على سبيل المثال sbsadmin).
2. حدد مكان التصحيح الذي تم تنزيله على النظام.
3. انقل مُثبّت التصحيح إلى مجلد `C:\Illumina` (مُعفى من نهج تقييد البرامج).
4. انقر نقرًا مزدوجًا على أيقونة المُثبّت لتشغيل الواجهة.

5. سيكشف المُثبّت تلقائيًا ما إذا تم تطبيق أداة التكوين من قبل أم لا و سيعرض خيارات جديدة:
   a. Change (تغيير): معتم و غير متوفر
   b. Repair (إصلاح): إصلاح الأخطاء و عرض خيارات لإعادة التكوين.
   c. Remove (إزالة): إلغاء تثبيت التصحيح و استعادة التكوين الافتراضي له (راجع *إلغاء التثبيت* على الصفحة 4)
6. في شاشة Installation Completion (إكمال عملية التثبيت)، حدد **Finish** (إنهاء).

إذا كان يلزم التحقق من تقرير التثبيت، فيُرجى مراجعة قسم *التحقق* على الصفحة 4.

يوصى بإعادة التشغيل في نهاية التثبيت.

إلغاء التثبيت

ستُعيد عملية إلغاء تثبيت التصحيح التعديلات التي تم إجراؤها على ملف تكوين مضيف التطبيق.

1. سجّل الدخول إلى النظام عبر حساب مسؤول (على سبيل المثال sbsadmin).
2. حدد مكان التصحيح الذي تم تنزيله على النظام.
3. انقل مُثبّت التصحيح إلى مجلد `C:\Illumina` (مُعفى من نهج تقييد البرامج).
4. انقر نقرًا مزدوجًا على أيقونة المُثبّت لتشغيل الواجهة.
5. حدد **Remove** (إزالة) لإلغاء تثبيت التصحيح و استعادة جميع القيم إلى الإعدادات الافتراضية.
6. حدد **Remove** (إزالة) للتحقق من خيار إلغاء تثبيت التصحيح و استعادة جميع القيم إلى الإعدادات الافتراضية.

سيعرض هذا الإعداد النظام باعتباره غير آمن و عُرضة لخطر الهجوم. يُوصى بشدة بمعالجة أي آثار تقنية تتسبب في خيار إزالة التصحيح قبل اختيار إلغاء التثبيت.

7. في شاشة Installation Completion (إكمال عملية التثبيت)، حدد **Finish** (إنهاء).

إذا كان يلزم التحقق من تقرير التثبيت، فيُرجى مراجعة قسم *التحقق* على الصفحة 4.

يوصى بإعادة التشغيل في نهاية التثبيت.

التحقق

إذا كانت هناك حاجة للتحقق من عملية التثبيت، فسيُنشَأ ملف التحقق متضمنًا التاريخ والطابع الزمني، وإصدار برنامج مدير التشغيل المحلي مُثبتًا، والقيم الرئيسية الأخرى الخاصة بعملية التحقق. للحصول على هذا الملف، يُرجى التواصل مع techsupport@illumina.com.

توصيات إضافية للأمان والتخفيف من المخاطر

يعتمد النشر الآمن لأجهزة RUO والأجهزة الطبية Dx على طبقات الأمان. توصي Illumina بشدة بتوزيع المعدات والأجهزة في أصغر شبكة فرعية أو سياق أمان للشبكة إلى جانب الأجهزة الموثوق بها. كما يُنصح بشدة باستخدام جدران الحماية ونُهج الشبكة الأخرى لتقييد عمليات الوصول الواردة والصادرة الأخرى.

نوصي أيضًا بما يلي:

- قم بتمكين بروتوكول أمان طبقة النقل (TLS) لضمان تشفير جميع الاتصالات خارج الجهاز.
  - لتمكين بروتوكول أمان طبقة النقل (TLS)، يُرجى الرجوع إلى دليل برنامج مدير التشغيل المحلي.

خيارات بديلة

إذا لم يكن تنفيذ التصحيح خيارًا لسببٍ ما، فقد تعمل طرق التخفيف اليدوية التالية على تقليل المخاطر:

- قم بتعطيل الوصول عن بُعد إلى برنامج مدير التشغيل المحلي عن طريق إضافة قواعد جدار الحماية لنظام التشغيل Windows لحظر اتصالات المنفذين 80 و443 الواردة.

سيقوم مُثبّت MSI بحظر الاتصالات الواردة عن بُعد تلقائيًا في تكوين خادم الويب الخاص ببرنامج مدير التشغيل المحلي. أحد إجراءات التخفيف اليدوية من المخاطر التي تحقق النتيجة نفسها هو تطبيق تكوين جدار الحماية لنظام التشغيل Windows، وذلك لحظر الاتصالات الواردة إلى اتصالات HTTP (TCP:80) و(HTTPS (TLS, TCP:443.

وبمجرّد التطبيق، لا يُمكن الوصول إلى برنامج مدير التشغيل المحلي إلا من خلال جهاز الكمبيوتر المُثبّت عليه مدير التشغيل المحلي؛ ولن يكون الوصول إليه من خلال أجهزة الكمبيوتر الأخرى المتصلة بالشبكة نفسها ممكنًا بعد ذلك.

إذا كان سير عمل المستخدم يتضمّن الوصول عن بُعد إلى برنامج مدير التشغيل المحلي، فلن تعمل هذه الوظيفة بعد الآن.

- قم بخفض عدد أجهزة الشبكة الأخرى إلى الحد الأدنى.

سيعمل تكوين الشبكة بحيث يتم خفض عدد أجهزة الشبكة الأخرى التي يُمكنها الاتصال بالأجهزة المتضررة إلى الحد الأدنى على تقليل آثار تلك الأجهزة. كلما كان عدد الاتصالات المتاحة للنظام أقل، أصبحت الفرص المتاحة لإمكانية الوصول أقل.

وقد يتطلب هذا التشاور مع موارد أمن المعلومات المحلي أو تكنولوجيا المعلومات لديك للتطبيق.

- أخرج الجهاز من الشبكة.

إذا لم يكن هناك خيار آخر ممكن، فإن التخفيف النهائي من المخاطر يتمثل في إخراج الجهاز من الشبكة بأكملها. سيعمل ذلك على تعطيل الوصول إلى خدمات Illumina Cloud/SaaS مثل عمليات سير عمل الخدمة الاستباقية ومركز التسلسل BaseSpace®، وعمليات سير العمل المتعلقة بتفريغ البيانات الجينومية النموذجية.

وقد يتطلب هذا التشاور مع موارد أمن المعلومات المحلي أو تكنولوجيا المعلومات لديك للتطبيق.

التحقيق في الوصول المحتمل غير المصرح به

قد تساعد الخطوات التالية مشغل الجهاز في تحديد ما إذا كان مستخدم غير مصرح له قد قام بالوصول إلى النظام:

1. فحص سجلات خدمات معلومات الإنترنت (IIS) المخزنة في C:\inetpub\logs\LogFiles\W3SVC1 بحثًا عن الاستدعاءات غير الطبيعية.
   - تظهر الاستدعاءات الطبيعية لخادم الويب الخاص ببرنامج مدير التشغيل المحلي على النحو التالي:

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

   - قد تظهر المكالمات غير الطبيعية لخادم الويب الخاص ببرنامج مدير التشغيل المحلي ، على سبيل المثال، على النحو التالي:

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

2. فحص سجل خدمات معلومات الإنترنت (IIS) بحثًا عن علامات عمليات تحميل POST لمحتوى غير ملفات البيان. على سبيل المثال، تشير الاستدعاءات التالية إلى وجود نشاط مريب:

```
wscript
```

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

3. إذا تم تثبيت تطبيق مكافحة الفيرو سات/مكافحة البرمجيات الضارة، فتحقق من سجلات البرنامج بحثًا عن علامات للسلوك غير الطبيعي.
4. فحص سجلات windows بحثًا عن علامات ر سائل خطأ غير طبيعية.

إذا تمكن أحد العناصر المُهددة من الوصول إلى حقوق المسؤول، فستكون لديه القدرة على تعديل جميع سجلات وأحداث الأجهزة المحلية أو حذفها.

تحقق من وجود أي نقاط نهاية قد حاول النظام الوصول إليها. وللحصول على قائمة بالاتصالات الصادرة المتوقعة، راجع جدار حماية كمبيوتر التحكم.

تواصل مع الدعم الفني لشركة Illumina للحصول على المساعدة المطلوبة.

تاريخ المراجعة

المستند	التاريخ	وصف التغيير
المستند رقم 200017330 v02	أبريل 2022	تمت إضافة توصية لتطبيق التصحيح عند عدم تشغيل الأداة. تمت إضافة تعليمات تفيد بأن إعادة تشغيل الجهاز مطلوبة بعد تثبيت التصحيح. تم تصحيح وصف محفوظات المراجعة للإصدار 01.
المستند رقم 200017330 الإصدار 01	أبريل 2022	تغير عنوان المستند إلى دليل إرشادات LRM Software Patch 1.0. تمت إزالة أي ذكر لـ v1.0.1. تمت إضافة قسم لتغطية التحقيق في الوصول غير المصرح به المحتمل.
المستند رقم 200017330 الإصدار 00	مارس 2022	الإصدار المبدئي.