illumina®

תיקון 1.0 לתוכנה LRM

מדריך הוראות

מבוא

לחברת Illumina® נודע על קיומה של פגיעות אבטחה בתוכנה Local Run Manager, והיא מספקת תיקון תוכנה כדי להגן מפני ניצול מרחוק של פגיעות זו.

Local Run Manager הוא יישום תוכנה עצמאי אשר מהווה חלק מתצורת ברירת המחדל של המערכות הבאות:

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

*לאבחון חוץ-גופי בלבד.

מדריך זה מתייחס למכשירי Illumina שפורטו לעיל, וכן למחשבים שאינם כוללים את המכשירים, שמותקנת בהם הגרסה העצמאית של Local Run Manager.

הפגיעות היא הרצת פקודה מרחוק (RCE) שאינה מאומתת, עם ציון CVSS ללא מזעור סיכונים של 10.0 - קריטי, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H`.

שלבי מזעור הסיכונים הבאים נדרשים במכשירים שפורטו לעיל, כדי להגן מפני אפשרות שבה משתמש בלתי-מורשה ייגש למכשיר אחד או יותר ויפעיל התקפה בגישה מרחוק.

אם, מסיבה כלשהי, לא ניתן להפעיל את תוכנית ההתקנה, עיין בסעיף מזעור הסיכונים הנוספים שבסוף מסמך זה או פנה לכתובת techsupport@illumina.com לקבלת סיוע נוסף.

ראה קבלת העדכון של Local Run Manager לקבלת אפשרויות כיצד להוריד או לבקש עותק של התיקון.

- **טלאי v1.0.0** - יעדכן את תצורת הרשת של Local Run Manager וישבית את הגישה מרחוק אל שירותי מידע באינטרנט (IIS).

קבלת תיקון האבטחה של Local Run Manager

יש ארבע (4) אפשרויות לקבלת תיקון האבטחה של Local Run Manager.

אפשרות **1**—הורדה ישירות למכשיר שלך

הדרך המהירה ביותר לקבל את עדכון האבטחה של Local Run Manager היא להוריד ישירות מאתר האינטרנט המארח אל המכשיר.

1. הורד את תוכנית ההתקנה של התיקון דרך הקישור שנשלח בהודעת דוא"ל מאובטחת למכשיר שלך.
2. העבר את הקובץ לתיקייה `C:\Illumina` במכשיר.
3. פעל בהתאם להוראות בסעיף *החלת תיקון האבטחה של Local Run Manager* בעמוד 3.

אפשרות **2**—הורדת תוכנית ההתקנה של התיקון אל המחשב והעברתה למכשיר באמצעות כונן **USB**/תיקייה משותפת

אם אינך מצליח להוריד את תיקון האבטחה למכשיר, אנו ממליצים להוריד למחשב נפרד ולאחר מכן להעבירו למכשיר.

לפני שתשתמש בכונן ה-USB, ודא את תקינותו מול נציגי האבטחה שלך. (מומלץ)

1. הורד את תוכנית ההתקנה של התיקון דרך הקישור שנשלח בהודעת דוא"ל מאובטחת, למחשב או למחשב הנייד שלך.
2. העתק את תוכנית ההתקנה של התיקון שהורדת, מהמחשב לכונן ה-USB או לתיקייה משותפת.
3. אם אתה משתמש בכונן USB, חבר את הכונן למכשיר.
4. העתק את תוכנית ההתקנה של התיקון מכונן ה-USB או מהתיקייה המשותפת אל התיקייה `C:\Illumina` במכשיר.
5. פעל בהתאם להוראות בסעיף *החלת תיקון האבטחה של Local Run Manager* בעמוד 3.

אפשרות **3**—בקשת תמיכה טכנית

נציג תמיכה טכנית של Illumina ינחה אותך לאורך תהליך התיקון באחת מהשיטות הבאות:

- התחברות מרחוק של התמיכה הטכנית
  נציג תמיכה טכנית ייגש מרחוק לכלי הניתוח ויתקין את התיקון בשם הלקוח.

  תידרש אפשרות לגשת למחשב מרחוק. אם יש לך שאלות כלשהן, פנה לנציג ה-IT בארגון לקבלת סיוע.

- הוראות עם הדרכה
  נציג תמיכה טכנית יספק הוראות והדרכה דרך הטלפון. אנא פנה לנציג התמיכה הטכנית באזורך לקבלת סיוע.

אפשרות **4**—הזמנת כונן שתצורתו הוגדרה מראש מ-**Illumina**

הלקוח יכול להזמין כונני USB מוגנים מפני כתיבה ללא עלות. כדי להזמין את הכונן שבו מותקן התיקון, אנא פנה לכתובת techsupport@illumina.com.

ייתכנו עיכובים במשלוח או במצאי, אשר עשויים להשפיע על לוחות זמני האספקה. כדי להגן על המערכות בצורה מיידית יותר, מומלץ מאוד להגן על המערכות בשיטה שתציע את נתיב הפתרון היעיל ביותר.

החלת תיקון האבטחה של Local Run Manager - תוכנית ההתקנה של גרסת v.1.0

הפעלה של Illumina MSI (Microsoft Installer) תעדכן את תצורת שרת האינטרנט של Local Run Manager כדי למנוע הפעלה של תוכן שהועלה על-ידי המשתמש ותחסום כל גישה מרחוק אל ממשק האינטרנט של Local Run Manager דרך חיבורי רשת LAN.

עבור משתמשים שמשתמשים בממשק האינטרנט של Local Run Manager כדי לגשת מרחוק למכשירים, זרימת עבודה זו תפסיק לפעול אחרי ההתקנה של תיקון זה. Illumina מתכננת לתקן את הבעיה ולשחזר פונקציונליות זו באמצעות תיקון תוכנה קבוע שייצא מאוחר יותר. אם בעיה זו מפריעה לזרימות העבודה שהתבססו כבר, אנא פנה לכתובת techsupport@illumina.com לקבלת סיוע נוסף.

תוכנית ההתקנה של MSI רלוונטית לכל הגרסאות של Local Run Manager ותקבע אוטומטית מהו התיקון הנכון על-פי הגרסה של Local Run Manager שמותקנת במכשיר/במחשב.

בנוסף, תוכנית התקנה זו של MSI תיצור קובץ ביקורת המראה שמזעור סיכונים זה הוטמע, יחד עם חותמת זמן כדי לשקף התקנה נאותה.

הפעלת תוכנית ההתקנה של MSI – בפעם הראשונה שמפעילים את תוכנית ההתקנה של MSI, תוכנית ההתקנה תתקן את המערכת ותיצור קובץ ביקורת הכולל את שעת השלמת הפעולה.

הפעלת תוכנית הפעולה של MSI פעם נוספת תיצור אפשרות **Repair** (תיקון), שבה המשתמש יכול להחיל את הטלאי מחדש או לבטלו ולחזור למצב הקודם. שים לב: ביטול התיקון וחזרה למצב הקודם יובילו לקבלת תצורת מכשירים לא מאובטחת.

החלת תיקון האבטחה של Local Run Manager

כדי להתקין את התיקון:

1. התחבר למערכת עם חשבון מנהל מערכת (למשל sbsadmin).

Illumina ממליצה להחיל את התיקון כשהמכשיר אינו מופעל. אם המכשיר צפוי לפעול, יש להחיל את התיקון מיד לאחר שפעולתו מסתיימת.

2. אתר את התיקון שהורד למערכת.
3. העבר את תוכנית ההתקנה של התיקון לתיקייה `C:\Illumina` (פטור ממדיניות הגבלת תוכנה).
4. לחץ לחיצה כפולה על סמל תוכנית ההתקנה כדי להפעיל את הממשק.
5. כאשר היישום נטען, בחר **Next** (הבא) כדי להתחיל בהתקנת התיקון.

6. במסך השלמת ההתקנה בחר **Finish** (סיום).

אם נדרש דוח אימות התקנה, ראה *אימות* בעמוד 5.

יש לבצע אתחול מחדש לאחר ההתקנה.

תיקון

אם אירעה שגיאה, הלקוח יכול לפעול בהתאם להוראות הבאות כדי לתקן את ההתקנה:

1. התחבר למערכת עם חשבון מנהל מערכת (למשל sbsadmin).
2. אתר את התיקון שהורד למערכת.
3. העבר את תוכנית ההתקנה של התיקון לתיקייה `C:\Illumina` (פטור ממדיניות הגבלת תוכנה).
4. לחץ לחיצה כפולה על סמל תוכנית ההתקנה כדי להפעיל את הממשק.
5. תוכנית ההתקנה תזהה אוטומטית אם כלי הגדרת התצורה הופעל קודם לכן ותציג אפשרויות חדשות:
   a. Change (שינוי): מופיעה באפור ולא זמינה
   b. Repair (תיקון): מתקנת שגיאות ומאפשרת הגדרה מחדש של התצורה.
   c. Remove (הסרה): הסרת התיקון ושחזור התצורה שנקבעה כברירת מחדל (ראה *הסרת התקנה* בעמוד 4)
6. במסך השלמת ההתקנה בחר **Finish** (סיום).

אם נדרש דוח אימות התקנה, ראה *אימות* בעמוד 5.

יש לבצע אתחול מחדש לאחר ההתקנה.

הסרת התקנה

הסרת ההתקנה של התיקון תבטל את השינויים שבוצעו בקובץ הגדרות התצורה של מארח היישום.

1. התחבר למערכת עם חשבון מנהל מערכת (למשל sbsadmin).
2. אתר את התיקון שהורד למערכת.
3. העבר את תוכנית ההתקנה של התיקון לתיקייה `C:\Illumina` (פטור ממדיניות הגבלת תוכנה).
4. לחץ לחיצה כפולה על סמל תוכנית ההתקנה כדי להפעיל את הממשק.
5. בחר **Remove** (הסר) כדי להסיר את התיקון ולהחזיר את כל הערכים להגדרות ברירת המחדל.
6. בחר **Remove** (הסר) כדי לאמת את אפשרות הסרת ההתקנה של התיקון והחזרת כל הערכים להגדרות ברירת המחדל.

הגדרה זו תעמיד את המערכת במצב לא מאובטח ובסיכון להתקפה. לפני שתבחר באפשרות להסיר את ההתקנה, מומלץ מאוד שתטפל בכל ההשפעות הטכניות שמובילות אותך לאפשרות להסיר את התיקון.

7. במסך השלמת ההתקנה בחר **Finish** (סיום).

אם נדרש דוח אימות התקנה, ראה *אימות* בעמוד 5.

מומלץ לבצע אתחול מחדש לאחר ההתקנה.

אימות

אם יש צורך לאמת את ההתקנה, יופק קובץ אימות שכולל את התאריך וחותמת הזמן, גרסת Local Run Manager שמותקנת, וערכי אימות מרכזיים נוספים. לקבלת קובץ זה אנא פנה לכתובת techsupport@illumina.com.

המלצות נוספות לשיפור האבטחה ומזעור הסכנה

פריסה מאובטחת של מכשירים המיועדים לשימוש מחקרי בלבד (RUO) ושל מכשירים רפואיים המשמשים לאבחון (Dx) תלויה בשכבות האבטחה. Illumina ממליצה מאוד לפרוס את המכשירים וההתקנים ברשת-המשנה או קונטקסט האבטחה הקטנים ביותר האפשריים, עם התקנים מהימנים. כדאי מאוד גם להשתמש בחומות אש או במדיניות רשת אחרת לצורך הגבלת הגישה לתוך הרשת או ביציאה ממנה.

המלצות נוספות:

- הפעל אבטחת שכבת תעבורה (TLS) כדי לוודא שכל התקשורת מחוץ למכשיר מוצפנת.
  - כדי להפעיל אבטחת שכבת תעבורה (TLS) אנא עיין במדריך התוכנה של Local Run Manager.

אפשרויות חלופיות

אם, מסיבה כלשהי, הפעלת תיקון התוכנה לא מתאפשרת, ניתן להפחית את הסיכון בעזרת השיטות הידניות הבאות:

- השבת את הגישה מרחוק אל Local Run Manager על-ידי הוספת כללי חומת אש של Windows כדי לחסום חיבורים נכנסים ביציאות 80 ו-443.
  תוכנית ההתקנה של MSI תחסום אוטומטית את החיבורים המרוחקים הנכנסים בתצורת שרת האינטרנט של Local Run Manager. מזעור סיכונים ידני שיוביל לתוצאה דומה הוא הטמעה של תצורת חומת אש של Windows לצורך חסימת חיבורים נכנסים אל החיבורים `TCP:80` (HTTP) ו-`TCP:443` (HTTPS, TLS).
  לאחר ההטמעה, ניתן יהיה לגשת אל Local Run Manager רק דרך המחשב שבו Local Run Manager מותקן; יותר לא תתאפשר גישה ממחשבים אחרים שמחוברים לאותה רשת.

> אם זרימת העבודה של המשתמש כוללת גישה מרחוק אל Local Run Manager, פונקציונליות זו לא תעבוד יותר.

- הקטן למינימום את מספר המכשירים האחרים ברשת.
  הגדרת תצורת הרשת באופן שיפחית למינימום את מספר המכשירים האחרים ברשת שמסוגלים לנהל תקשורת עם המכשיר שהושפע, תצמצם את פוטנציאל הניצול. ככל שיהיו פחות חיבורים זמינים במערכת, כך יהיו פחות הזדמנויות זמינות לגישה.
  ייתכן ששיטה זו תחייב התייעצות עם גורמי אבטחת המידע או ה-IT בארגון.
- הוצא את המכשיר מהרשת.

אם אין אפשרות אחרת, שיטת מזעור הסיכונים הסופית היא הוצאה מוחלטת של המכשיר מהרשת. פעולה זו תשבית את הגישה לשירותי הענן/ה-SaaS של Illumina, כגון Proactive ו-BaseSpace® Sequence Hub, וזרימות עבודה טיפוסיות של פריקת נתונים גנומיים.
ייתכן ששיטה זו תחייב התייעצות עם גורמי אבטחת המידע או ה-IT בארגון.

חקירת אפשרות לגישה בלתי-מורשית

השלבים הבאים עשויים לסייע למפעיל המכשיר לקבוע אם משתמש בלתי-מורשה ניגש למערכת:

1. בדוק את יומני ה-IIS המאוחסנים בכתובת `C:\inetpub\logs\LogFiles\W3SVC1` כדי לזהות בהם קריאות חריגות.
   - הקריאות הרגילות לשרת האינטרנט של Local Run Manager נראות כך:

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

   - קריאות חריגות לשרת האינטרנט של Local Run Manager עשויות להיראות, לדוגמה, כך:

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

2. בדוק את היומן של IIS לאיתור סימני העלות תוכן POST שאינן קובצי מניפסט. לדוגמה, הקריאות הבאות עשויות להעיד על פעילות חשודה:

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

3. אם מותקן יישום אנטי וירוס/אנטי תוכנה זדונית כלשהו, עיין ביומני התוכנה לזיהוי סימנים לפעילות חריגה.
4. בדוק את היומנים של Windows לזיהוי סימנים להודעות על שגיאות חריגות.
   אם גורם מאיים כלשהו קיבל גישה עם זכויות מנהל מערכת, הוא יוכל לשנות או למחוק את כל האירועים ויומני המכשירים המקומיים.

בדוק אם קיימות במערכת נקודות קצה כלשהן שבהן נעשו ניסיונות גישה. לקבלת רשימת החיבורים היוצאים הצפויים, עיין בחומת האש של מכשיר הבקרה.

אם יש לך צורך בסיוע, פנה לתמיכה הטכנית של Illumina.

גרסאות קודמות

מסמך	תאריך	תיאור השינוי
מסמך מס' 200017330 v02	אפריל 2022	נוספה המלצה להחיל תיקון כאשר המכשיר אינו בפעולה. נוספה הוראה הקובעת שנדרש אתחול מחדש של המכשיר לאחר התקנת התיקון. תוקן תיאור המהדורות הקודמות של v01.
מסמך מס' 200017330 v01	אפריל 2022	כותרת המסמך שונתה ל'מדריך הוראות לתיקון 1.0 לתוכנה LRM'. כל האזכורים של גרסה v1.0.1 הוסרו. נוסף סעיף הדן בחקירה של אפשרות לגישה בלתי-מורשית.
מסמך מס' 200017330 v00	מרץ 2022	מהדורה ראשונית.