Oprava softwaru LRM verze 1.0

illumina®

Návod k použití

Úvod

Společnost Illumina® zjistila bezpečnostní chybu v softwaru Local Run Manager a poskytla softwarovou opravu, která chrání před vzdáleným zneužitím této chyby

Local Run Manager je samostatná softwarová aplikace, která je součástí výchozí konfigurace v následujících systémech:

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

Určeno k diagnostice in vitro.

Tato příručka se vztahuje na přístroje Illumina uvedené výše a také na počítače mimo přístroj, na kterých je nainstalována samostatná verze softwaru Local Run Manager.

Jde o chybu neautorizovaného vzdáleného spouštění příkazů (Unauthenticated Remote Command Execution, RCE), jejíž skóre CVSS bez opravy je 10,0 – kritické, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H`.

Na všech přístrojích uvedených výše jsou potřeba provést následující opatření pro zabezpečení proti tomu, aby mohl neoprávněný uživatel získat přístup k jednomu nebo více přístrojům a provést útok vzdáleným přístupem.

Pokud z nějakého důvodu nelze instalační program spustit, podívejte se do kapitoly o dalších bezpečnostních opatřeních na konci tohoto dokumentu nebo si vyžádejte další pomoc na adrese techsupport@illumina.com.

Možnosti stažení nebo vyžádání kopie opravy naleznete v kapitole Získání aktualizace modulu Local Run Manager.

- **Oprava verze v1.0.0** – aktualizuje webovou konfiguraci modulu Local Run Manager a zakáže vzdálený přístup k internetovým informačním službám (Internet Information Services, IIS).

Získání bezpečnostní opravy modulu Local Run Manager

Existují čtyři (4) možnosti získání bezpečnostní opravy modulu Local Run Manager.

Možnost 1 – Přímé stažení do přístroje

Nejrychlejší způsob, jak získat bezpečnostní aktualizaci modulu Local Run Manager, je stáhnout si ji z hostitelské webové stránky přímo do přístroje.

1. Instalační program opravy si stáhněte prostřednictvím odkazu, který vám přijde zabezpečeným e-mailem do vašeho přístroje.
2. Přesuňte soubor do složky `C:\Illumina` v přístroji.
3. Postupujte podle pokynů v kapitole *Použití bezpečnostní opravy modulu Local Run Manager* na straně 4.

Možnost 2 – Stažení instalačního programu opravy do počítače a jeho přesun do přístroje prostřednictvím USB disku nebo sdílené složky

Pokud nemůžete stáhnout bezpečnostní opravu do přístroje, doporučujeme ji stáhnout do samostatného počítače a poté přenést do přístroje.

Před použitím USB disku si ověřte jeho neporušenost u svých pracovníků pro bezpečnost. (doporučeno).

1. Instalační program opravy si stáhněte prostřednictvím odkazu, který vám přijde zabezpečeným e-mailem do vašeho počítače nebo notebooku.
2. Stažený instalační program opravy zkopírujte z počítače na USB disk nebo do sdílené složky.
3. Pokud použijete USB disk, vložte jej do přístroje.
4. Stažený instalační program opravy zkopírujte z USB disku nebo sdílené složky do složky `C:\Illumina` v přístroji.
5. Postupujte podle pokynů v kapitole *Použití bezpečnostní opravy modulu Local Run Manager* na straně 4.

Možnost 3 – Žádost o technickou podporu

Zástupce technické podpory společnosti Illumina vás provede postupem opravy některým z následujících způsobů:

- Vzdálené přihlášení technické podpory
  Zástupce technické podpory získá vzdálený přístup do analyzátoru a nainstaluje opravu za zákazníka.

  Systém musí umožňovat vzdálený přístup. V případě dotazů požádejte o pomoc svého místního pracovníka IT.

- Postup podle pokynů
  Zástupce technické podpory poskytne pokyny po telefonu. O pomoc se obraťte na svého místního zástupce technické podpory.

Možnost 4 – Objednání předem nakonfigurovaného disku od společnosti Illumina

Zákazník si může bezplatně objednat USB disky chráněné proti zápisu. Disk s nainstalovanou opravou si můžete vyžádat na adrese techsupport@illumina.com.

V expedici nebo skladu může dojít ke zpožděním, která ovlivní včasnost dodávky. Aby byly systémy ochráněny rychleji, důrazně doporučujeme využít způsob, který zajistí nejefektivnější cestu k řešení.

Použití instalačního programu bezpečnostní opravy modulu Local Run Manager verze v.1.0

Instalační program MSI (Microsoft Installer) společnosti Illumina po spuštění aktualizuje konfiguraci webového serveru modulu Local Run Manager tak, aby zabránil spuštění jakéhokoli uživatelem nahraného obsahu a zablokoval veškerý vzdálený přístup k webovému rozhraní modulu Local Run Manager ze sítí LAN.

Pro uživatele, kteří používají webové rozhraní modulu Local Run Manager pro vzdálený přístup k přístrojům, přestane tento pracovní postup po instalaci této opravy fungovat. Společnost Illumina chce tuto funkci obnovit později pomocí trvalé softwarové opravy tohoto problému. Pokud instalace opravy způsobí přerušení zavedených pracovních postupů, kontaktujte technickou podporu společnosti Illumina (techsupport@illumina.com) a požádejte o další pomoc.

Instalační program MSI je určen pro všechny verze modulu Local Run Manager a automaticky zjistí správnou opravu na základě verze modulu Local Run Manager nainstalované v přístroji/počítači.

Tento instalační program MSI také vytvoří kontrolní soubor, který dokládá, že byla tato oprava zavedena, spolu s časovým razítkem potvrzujícím správnou instalaci.

Spuštění instalačního programu MSI – při prvním spuštění instalačního programu MSI instalační program opraví systém a vytvoří kontrolní soubor s časem dokončení.

Při opětovném spuštění instalačního programu MSI se zobrazí možnost **Repair** (Oprava). Uživatel má možnost opravu znovu použít nebo odinstalovat. Poznámka: Odinstalace opravy bude mít za následek, že konfigurace přístroje nebude zabezpečená.

Použití bezpečnostní opravy modulu Local Run Manager

Instalace opravy:

1. Přihlaste se do systému prostřednictvím účtu správce (např. sbsadmin).

   Společnost Illumina doporučuje, aby byla oprava instalována, když není přístroj spuštěn. Pokud přístroj provádí běh, měla by být oprava instalována ihned po dokončení běhu.

2. Vyhledejte opravu staženou do systému.
3. Přesuňte instalační program opravy do složky `C:\Illumina` (výjimka ze zásad omezení softwaru).
4. Poklepáním na ikonu instalačního programu otevřete rozhraní.
5. Až se aplikace načte, výběrem možnosti **Next** (Další) spusťte instalaci opravy.
6. Na obrazovce dokončení instalace vyberte **Finish** (Dokončit).

Pokud je vyžadováno ověření instalačního protokolu, podívejte se do části *Ověření* na straně 5.

Na konci instalace je nutné přístroj restartovat.

Oprava

V případě výskytu chyby může zákazník provést opravu instalace podle následujících pokynů:

1. Přihlaste se do systému prostřednictvím účtu správce (např. sbsadmin).
2. Vyhledejte opravu staženou do systému.
3. Přesuňte instalační program opravy do složky `C:\Illumina` (výjimka ze zásad omezení softwaru).
4. Poklepáním na ikonu instalačního programu otevřete rozhraní.
5. Instalační program automaticky zjistí, jestli už byl konfigurační nástroj dříve použit, a nabídne nové možnosti:
   a. Change (Změnit): Možnost je zbarvená šedě a není k dispozici
   b. Repair (Opravit): Umožňuje opravit chyby a nabízí možnosti pro změnu konfigurace.
   c. Remove (Odebrat): Umožňuje odinstalovat opravu a obnovit výchozí konfiguraci (viz *Odinstalace* na straně 5)
6. Na obrazovce dokončení instalace vyberte **Finish** (Dokončit).

Pokud je vyžadováno ověření instalačního protokolu, podívejte se do části *Ověření* na straně 5.

Na konci instalace je nutné přístroj restartovat.

Odinstalace

Odinstalací opravy se vrátí zpět všechny úpravy provedené v konfiguračním souboru hostitelské aplikace.

1. Přihlaste se do systému prostřednictvím účtu správce (např. sbsadmin).
2. Vyhledejte opravu staženou do systému.
3. Přesuňte instalační program opravy do složky `C:\Illumina` (výjimka ze zásad omezení softwaru).
4. Poklepáním na ikonu instalačního programu otevřete rozhraní.
5. Výběrem možnosti **Remove** (Odebrat) se oprava odinstaluje a všechny hodnoty se vrátí do výchozích nastavení.
6. Výběrem možnosti **Remove** (Odebrat) potvrdíte odinstalaci opravy a vrácení všech hodnot do výchozích nastavení.

Při tomto nastavení zůstane systém nezabezpečený a bude vystaven riziku úroku. Důrazně se doporučuje před odinstalací vyřešit všechny technické aspekty, které vedly k rozhodnutí opravu odebrat.

7. Na obrazovce dokončení instalace vyberte **Finish** (Dokončit).

Pokud je vyžadováno ověření instalačního protokolu, podívejte se do části *Ověření* na straně 5.

Na konci instalace se doporučuje přístroj restartovat.

Ověření

Pokud bude potřeba instalaci ověřit, bude vygenerován ověřovací soubor obsahující datové a časové razítko, verzi nainstalovaného modulu Local Run Manager a další klíčové hodnoty pro ověření. Soubor si můžete vyžádat na adrese techsupport@illumina.com.

Další doporučení pro omezení rizik a zabezpečení

Bezpečné nasazení přístrojů v režimu výzkumu (RUO) a lékařských zařízení v diagnostickém režimu (Dx) závisí na jednotlivých vrstvách zabezpečení. Společnost Illumina důrazně doporučuje, aby byly přístroje a zařízení nasazeny v co nejmenší síťové podsíti nebo v zabezpečeném prostředí spolu s důvěryhodnými zařízeními. Důrazně se pak doporučuje používat firewally a další síťové postupy k omezení jiných příchozích a odchozích přístupů.

Další doporučení:

- Povolit protokol TLS (Transport Layer Security), aby byla veškerá komunikace mimo přístroj šifrována.
  - Informace o povolení protokolu TLS (Transport Layer Security) naleznete v příručce softwaru Local Run Manager.

Alternativní možnosti

Pokud zavedení opravy není z nějakého důvodu možné, snížíte riziko následujícími ručními opatřeními:

- Zakažte vzdálený přístup k modulu Local Run Manager přidáním pravidel brány firewall systému Windows, která zablokují příchozí připojení na portech 80 a 443.
  Instalační program MSI automaticky zablokuje vzdálená příchozí připojení v konfiguraci webového serveru modulu Local Run Manager. Ručním řešením, které dosáhne stejného výsledku, je implementace konfigurace brány firewall systému Windows, která blokuje příchozí připojení `HTTP (TCP:80)` a `HTTPS (TLS, TCP:443)`.
  Po zakázání přístupu bude modul Local Run Manager přístupný pouze na počítači, na kterém je nainstalován. Z jiných počítačů připojených ke stejné síti již přístupný nebude.

  Pokud pracovní postup uživatele zahrnuje vzdálený přístup k modulu Local Run Manager, nebude tato funkce již fungovat.

- Minimalizujte počet dalších síťových zařízení.
  Nastavením sítě tak, aby se minimalizoval počet dalších síťových zařízení, která mohou komunikovat s příslušným přístrojem, se sníží možnost zneužití. Čím menší je počet připojení k systému, tím méně je možností přístupu.
  Provedení tohoto nastavení může vyžadovat konzultaci s místním oddělením pro zabezpečení informací nebo IT.

- Odpojte přístroj od sítě.
  Pokud nelze použít jinou možnost, je krajním opatřením úplné odpojení přístroje od sítě. Tím bude znemožněn přístup ke službám Illumina Cloud/SaaS, jako jsou Proactive a BaseSpace® Sequence Hub, a k typickým pracovním postupům pro přenos genomových dat.
  Provedení tohoto nastavení může vyžadovat konzultaci s místním oddělením pro zabezpečení informací nebo IT.

Prověření možného neoprávněného přístupu

Následující kroky mohou obsluze přístroje pomoci zjistit, zda do systému nezískal přístup neoprávněný uživatel:

1. Zkontrolujte protokoly služby IIS uložené v `C:\inetpub\logs\LogFiles\W3SVC1` zda neobsahují neobvyklá volání.
   - Běžná volání na webový server Local Run Manager vypadají následovně:

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

   - Neobvyklá volání webového serveru Local Run Manager se mohou projevit například takto:

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

2. Zkontrolujte protokol služby IIS, zda neobsahuje známky odesílání jiného obsahu než souborů manifestů (POST). Na podezřelou aktivitu poukazují například následující volání:

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

3. Pokud máte nainstalovanou antivirovou nebo antimalwarovou aplikaci, zkontrolujte, zda protokoly softwaru nevykazují známky neobvyklého chování.
4. Zkontrolujte protokoly systému Windows, zda neobsahují známky neobvyklých chybových hlášení.
   Pokud by útočník získal přístup s právy správce, mohl by měnit nebo odstraňovat všechny protokoly a události místního přístroje.

Zkontrolujte, zda se systém nepokusil získat přístup ke koncovým bodům. Seznam očekávaných odchozích připojení naleznete v části Brána firewall řidicího počítače.

V případě potřeby se obraťte na technickou podporu společnosti Illumina.

Historie revizí

Dokument	Datum	Popis změny
Dokument č. 200017330 v02	Duben 2022	Bylo přidáno doporučení instalovat opravu, když není přístroj spuštěn. Byl přidán pokyn, že je po instalaci opravy nutné přístroj restartovat. Opraven popis historie revizí pro verzi v01.
Dokument č. 200017330 v01	Duben 2022	Byl změněn název dokumentu na Návod k použití pro opravu softwaru LRM verze 1.0. Byly odstraněny jakékoli zmínky o verzi 1.0.1. Byla přidána část týkající se prověřování případného neoprávněného přístupu.
Dokument č. 200017330 v00	Březen 2022	První vydání.