Popravek programske opreme LRM Software Patch 1.0

illumina®

Navodila za uporabo

Uvod

Družba Illumina® je seznanjena z varnostno ranljivostjo programske opreme Local Run Manager in zagotavlja popravek programske opreme za zaščito pred oddaljenim izkoriščanjem te ranljivosti.

Local Run Manager je samostojna programska aplikacija, ki je del privzete konfiguracije v naslednjih sistemih:

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

*Samo za diagnostično uporabo in vitro.

Ta navodila veljajo za zgoraj navedene instrumente in računalnike brez instrumenta družbe Illumina, v katerih je nameščena samostojna različica programske opreme Local Run Manager.

Nerazrešena ranljivost je nepooblaščeno oddaljeno izvajanje ukazov (RCE) z oceno sistema CVSS 10.0 Critical (Kritično), `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H`.

Spodnje korake za zmanjšanje tveganja je treba izvesti v zgoraj navedenih instrumentih za namene zaščite pred možnostjo nepooblaščenega dostopa uporabnika do enega ali več instrumentov ter izvedbe napada z oddaljenim dostopom.

Če namestitvenega programa iz kakšnega razloga ni mogoče zagnati, si oglejte razdelek z dodatnimi ukrepi za zmanjšanje tveganja na koncu tega dokumenta ali pa nam za dodatno pomoč pišite na naslov techsupport@illumina.com.

Možnosti za prenos ali pošiljanje zahteve za kopijo popravka so opisane v razdelku Pridobitev posodobitve za Local Run Manager.

- **Popravek v1.0.0** – posodobi spletno konfiguracijo programske opreme Local Run Manager in onemogoči oddaljen dostop do internetnih informacijskih storitev (IIS).

Pridobivanje varnostnega popravka za Local Run Manager

Varnostni popravek za Local Run Manager lahko pridobite na štiri (4) načine.

1. možnost – prenos neposredno v instrument

Varnostno posodobitev za Local Run Manager najhitreje pridobite tako, da jo prenesete neposredno z gostiteljskega spletnega mesta v instrument.

1. Prenesite namestitveni program popravka prek povezave, ki ste jo prejeli v varnem e-poštnem sporočilu, v svoj instrument.
2. Prenesite datoteko v mapo `C:\Illumina` v instrumentu.
3. Upoštevajte navodila v razdelku *Uporaba varnostnega popravka za Local Run Manager* na strani 4.

2. možnost – prenos namestitvenega programa popravka v računalnik in njegov prenos v instrument prek pogona USB/mape v skupni rabi

Če varnostnega popravka ne morete prenesti v instrument, priporočamo, da ga prenesete v ločen računalnik in ga nato prenesete v instrument.

Pred uporabo preverite celovitost pogona USB pri svojih zastopnikih za varnost. (Priporočeno)

1. Prenesite namestitveni program popravka prek povezave, ki ste jo prejeli v varnem e-poštnem sporočilu, v računalnik ali prenosnik.
2. Kopirajte preneseni namestitveni program popravka na pogon USB ali v mapo v skupni rabi v računalniku.
3. Če uporabljate pogon USB, ga priključite na instrument.
4. Kopirajte namestitveni program popravka iz pogona USB ali mape v skupni rabi v mapo `C:\Illumina` v instrumentu.
5. Upoštevajte navodila v razdelku *Uporaba varnostnega popravka za Local Run Manager* na strani 4.

3. možnost – pošiljanje zahteve za tehnično podporo

Predstavnik tehnične podpore družbe Illumina vas bo vodil skozi postopek popravljanja z enim od teh načinov:

- Oddaljena prijava predstavnika tehnične podpore
  Predstavnik tehnične podpore bo oddaljeno dostopal do analizatorja in namestil popravek v imenu stranke.

  V sistemu je treba omogočiti oddaljen dostop. Če imate kakršna koli vprašanja, se za pomoč obrnite na lokalnega predstavnika za IT.

- Vodena navodila
  Predstavnik tehnične podpore vam bo po telefonu posredoval vodena navodila. Za pomoč se obrnite na svojega lokalnega predstavnika tehnične podpore.

4. možnost – naročilo vnaprej konfiguriranega pogona pri družbi Illumina

Stranka lahko brezplačno naroči pogone USB, zaščitene pred zapisovanjem. Če želite naročiti pogon z nameščenim popravkom, nam pišite na naslov techsupport@illumina.com.

Pri pošiljkah ali zalogah lahko pride do zamud, ki lahko vplivajo na pravočasno dostavo. Močno priporočamo, da takoj zaščitite sisteme na način, ki zagotavlja najučinkovitejšo pot rešitve.

Uporaba namestitvenega programa za Local Run Manager Security Patch v.1.0

Namestitveni program Illumina MSI (Microsoft Installer) ob zagonu posodobi konfiguracijo spletnega strežnika Local Run Manager, da prepreči izvajanje kakršne koli vsebine, ki jo je naložil uporabnik, in blokira ves oddaljen dostop do spletnega vmesnika programske opreme Local Run Manager iz omrežnih povezav LAN.

Za uporabnike, ki za oddaljen dostop do instrumentov uporabljajo spletni vmesnik programske opreme Local Run Manager, ta delovni postopek po namestitvi tega popravka ne bo več deloval. Illumina namerava pozneje delovanje te funkcije znova omogočiti s trajnim popravkom programske opreme za to težavo. Če to povzroči prekinitev ustaljenih delovnih postopkov, za nadaljnjo pomoč pišite na naslov techsupport@illumina.com.

Namestitveni program MSI se uporablja za vse različice programske opreme Local Run Manager in samodejno določi pravilen popravek glede na različico programske opreme Local Run Manager, nameščene v instrumentu/računalniku.

Ta namestitveni program MSI bo ustvaril tudi revizijsko datoteko, ki prikazuje, da je bil ta ukrep za zmanjšanje tveganja izveden, in časovni žig, ki prikazuje pravilno namestitev.

Zagon namestitvenega programa MSI – namestitveni program MSI pri prvem zagonu popravi sistem in ustvari revizijsko datoteko s časom dokončanja.

Pri ponovnem zagonu namestitvenega programa MSI bo na voljo možnost **Repair** (Popravi), s katero lahko uporabnik znova uporabi popravek ali ga razveljavi. Opomba: konfiguracija instrumenta bo v primeru razveljavitve popravka nezanesljiva.

Uporaba varnostnega popravka za Local Run Manager

Upoštevajte spodnja navodila za namestitev popravka:

1. V sistem se prijavite s skrbniškim računom (npr. sbsadmin).

   Družba Illumina priporoča uporabo popravka v času, ko instrument ne deluje. Če se v instrumentu izvaja sekvenciranje, je treba popravek uporabiti takoj po dokončani izvedbi postopka sekvenciranja.

2. Poiščite popravek, ki ste ga prenesli v sistem.
3. Premaknite namestitveni program popravka v mapo `C:\Illumina` (ki je izvzeta iz pravilnika z omejitvami programske opreme).
4. Dvokliknite ikono namestitvenega programa, da zaženete vmesnik.
5. Ko se aplikacija naloži, izberite **Next** (Naprej), da začnete namestitev popravka.
6. Na zaslonu »Installation Completion« (Namestitev je dokončana) izberite **Finish** (Dokončaj).

Če potrebujete poročilo o preverjanju namestitve, glejte razdelek *Preverjanje* na strani 5.

Po končani namestitvi morate znova zagnati instrument.

Popravilo

Stranka lahko v primeru napake izvede popravilo namestitve v skladu s spodnjimi navodili:

1. V sistem se prijavite s skrbniškim računom (npr. sbsadmin).
2. Poiščite popravek, ki ste ga prenesli v sistem.
3. Premaknite namestitveni program popravka v mapo `C:\Illumina` (ki je izvzeta iz pravilnika z omejitvami programske opreme).
4. Dvokliknite ikono namestitvenega programa, da zaženete vmesnik.
5. Namestitveni program bo samodejno zaznal, ali je bilo orodje za konfiguracijo že zagnano, in prikazal nove možnosti:
   a. »Change« (Spremeni): zatemnjena in ni na voljo.
   b. »Repair« (Popravi): popravi napake in prikaže možnosti za ponovno konfiguracijo.
   c. »Remove« (Odstrani): odstrani popravek in ga obnovi v privzeto konfiguracijo (glejte *Odstranitev* na strani 5).
6. Na zaslonu »Installation Completion« (Namestitev je dokončana) izberite **Finish** (Dokončaj).

Če potrebujete poročilo o preverjanju namestitve, glejte razdelek *Preverjanje* na strani 5.

Po končani namestitvi morate znova zagnati instrument.

Odstranitev

Če odstranite popravek, razveljavite spremembe v konfiguracijski datoteki gostiteljske aplikacije.

1. V sistem se prijavite s skrbniškim računom (npr. sbsadmin).
2. Poiščite popravek, ki ste ga prenesli v sistem.
3. Premaknite namestitveni program popravka v mapo `C:\Illumina` (ki je izvzeta iz pravilnika z omejitvami programske opreme).
4. Dvokliknite ikono namestitvenega programa, da zaženete vmesnik.
5. Izberite **Remove (Odstrani)**, da odstranite popravek in ponastavite vse vrednosti na privzete nastavitve.
6. Izberite **Remove (Odstrani)**, da preverite možnost odstranitve popravka in ponastavite vse vrednosti na privzete nastavitve.

Sistem zaradi te nastavitve ne bo zaščiten in bo izpostavljen tveganju napada. Preden se odločite za odstranitev popravka, vam priporočamo, da odpravite morebitne tehnične težave, zaradi katerih je treba odstraniti popravek.

7. Na zaslonu »Installation Completion« (Namestitev je dokončana) izberite **Finish** (Dokončaj).

Če potrebujete poročilo o preverjanju namestitve, glejte razdelek *Preverjanje* na strani 5.

Priporočamo, da po končani namestitvi znova zaženete instrument.

Preverjanje

Če je treba preveriti namestitev, bo ustvarjena datoteka za preverjanje, ki bo vsebovala datumski in časovni žig, različico nameščene programske opreme Local Run Manager ter druge ključne vrednosti za preverjanje. Če želite pridobiti to datoteko, nam pišite na naslov techsupport@illumina.com.

Priporočila za dodatne ukrepe za zmanjšanje tveganja in izboljšanje varnosti

Varna uvedba instrumentov RUO in medicinskih pripomočkov Dx je odvisna od ravni varnosti. Illumina močno priporoča, da so instrumenti in pripomočki nameščeni v najmanjšem podomrežju omrežja ali varnostnem kontekstu z zaupanja vrednimi pripomočki. Zelo priporočljiva je uporaba požarnih zidov in drugih pravilnikov omrežja za omejitev drugih dohodnih in odhodnih dostopov.

Priporočamo tudi to:

- Omogočite protokol TLS (Transport Layer Security), da poskrbite za šifriranje vseh komunikacij zunaj instrumenta.

– Navodila za omogočanje protokola TLS (Transport Layer Security) najdete v navodilih za programsko opremo Local Run Manager.

Nadomestne možnosti

Če zagon popravka iz kakršnega koli razloga ni mogoč, lahko tveganje zmanjšate z naslednjimi ročnimi ukrepi za zmanjšanje tveganja:

- Onemogočite oddaljen dostop do programske opreme Local Run Manager tako, da dodate pravila požarnega zidu sistema Windows za blokiranje dohodnih povezav na vratih 80 in 443.
  Namestitveni program MSI bo v konfiguraciji spletnega strežnika Local Run Manager samodejno blokiral oddaljene dohodne povezave. Ročni ukrep za zmanjšanje tveganja, s katerim dosežete enak rezultat, je uvedba konfiguracije požarnega zidu sistema Windows za blokiranje dohodnih povezav za povezave `HTTP (TCP:80)` in `HTTPS (TLS, TCP:443)`.
  Po uvedbi je do dostop do programske opreme Local Run Manager mogoč samo prek računalnika, v katerem je nameščena programska oprema Local Run Manager, prek drugih računalnikov, ki imajo vzpostavljeno povezavo z istim omrežjem, pa dostop do programske opreme ne bo več mogoč.

Če delovni postopek uporabnika vključuje oddaljen dostop do programske opreme Local Run Manager, ta funkcija ne bo več delovala.

- Zmanjšajte število drugih omrežnih naprav.
  Če omrežje konfigurirate tako, da zmanjšate število drugih omrežnih naprav, ki lahko komunicirajo z zadevnim instrumentom, zmanjšate možnost izkoriščanja. Če je število povezav do sistema manjše, je na voljo tudi manj možnosti za dostop.
  Za izvedbo tega ukrepa se boste morda morali posvetovati z lokalnimi viri za informacijsko varnost ali IT.
- Odstranite instrument iz omrežja.
  Če ni na voljo nobena druga možnost, je zadnji ukrep za zmanjšanje tveganja ta, da instrument v celoti odstranite iz omrežja. S tem ukrepom boste onemogočili dostop do storitev Illumina Cloud/SaaS, kot sta Proactive in BaseSpace® Sequence Hub, ter običajnih delovnih postopkov za razbremenitev genomskih podatkov.
  Za izvedbo tega ukrepa se boste morda morali posvetovati z lokalnimi viri za informacijsko varnost ali IT.

Odkrivanje morebitnega nepooblaščenega dostopa

Z uporabo spodnjih korakov lahko upravljavec instrumenta lažje odkrije, ali je nepooblaščeni uporabnik morda dostopal do sistema:

1. Preverite, ali so v dnevnikih IIS, shranjenih v mapi `C:\inetpub\logs\LogFiles\W3SVC1`, zabeleženi morebitni neobičajni klici.
   - Običajni klici v spletnem strežniku Local Run Manager so videti tako:
     ```
     GET http /normalresource.extension?normal-URI-decoration
     ```
   - Neobičajni klici v spletnem strežniku Local Run Manager so lahko na primer videti tako:
     ```
     POST http /hackertool.asp
     ```
2. Preverite, ali so v dnevnikih IIS zabeležena morebitna nalaganja vsebine POST, ki niso manifestne datoteke. Ti klici na primer označujejo sumljivo dejavnost:
   ```
   wscript
   shell
   wscript.network
   scripting.filesystemObject
   ```
3. Če je nameščen protivirusni program/program za preprečevanje zlonamerne programske opreme, preverite, ali so v dnevnikih programske opreme zabeležena morebitna nenavadna vedenja.
4. Preverite, ali so v dnevnikih oken zabeležena morebitna nenavadna sporočila o napakah.
   Če je akter grožnje pridobil dostop s skrbniškimi pravicami, je lahko spremenil ali izbrisal vse lokalne dnevnike in dogodke v instrumentu.

Preverite morebitne končne točke, do katerih je sistem morda želel dostopati. Seznam morebitnih pričakovanih izhodnih povezav je na voljo v razdelku Požarni zid računalnika za nadzor.

Za pomoč se po potrebi obrnite na tehnično podporo družbe Illumina.

Zgodovina revizij

Dokument	Datum	Opis spremembe
Dokument št. 200017330 v02	April 2022	Dodano priporočilo za uporabo popravka, ko instrument ne deluje. Dodano navodilo, da je po namestitvi popravka potreben ponovni zagon instrumenta. Popravljen opis zgodovine revizij za različico v01.
Št. dokumenta 200017330 v01	April 2022	Spremenjen naslov dokumenta v »Navodila za uporabo za popravek programske opreme LRM Software Patch 1.0«. Odstranjene vse omembe v1.0.1. Dodan razdelek o odkrivanju morebitnega nepooblaščenega dostopa.
Dokument št. 200017330 v00	Marec 2022	Prva izdaja.