# Softverska zakrpa 1.0 za LRM

illumina®

Vodič s uputama

# Uvod

Illumina® je saznala za sigurnosnu ranjivost u softveru Local Run Manager i ponudila softversku zakrpu koja štiti od daljinskog iskorištavanja te ranjivosti.

Local Run Manager samostalna je softverska aplikacija i dio zadane konfiguracije sljedećih sustava:

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

*Za in vitro dijagnostiku.

Ovaj se priručnik odnosi na prethodno navedene instrumente, ali i na računala uz instrumente tvrtke Illumina na kojima je instalirana samostalna verzija softvera Local Run Manager.

Ranjivost se sastoji od neovlaštenog daljinskog izvršavanja naredbi (Unauthenticated Remote Command Execution, RCE) uz CVSS-ovu neublaženu ocjenu od 10,0, "Kritična", `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H`.

Na prethodno navedenim instrumentima potrebno je poduzeti sljedeće korake za ublažavanje kako bi se neovlaštenom korisniku onemogućio pristup jednom od instrumenata ili većem broju njih i izvođenje napada putem daljinskog pristupa.

Ako iz nekog razloga nije moguće izvršiti alat za instalaciju, pročitajte odjeljak s dodatnim mjerama ublažavanja pri kraju ovog dokumenta ili zatražite dodatnu pomoć putem adrese e-pošte techsupport@illumina.com.

U odjeljku Pribavljanje ažuriranja za Local Run Manager potražite mogućnosti kako preuzeti ili zatražiti primjerak zakrpe.

- **zakrpa v1.0.0** – ažurirat će web-konfiguraciju softvera Local Run Manager i onemogućiti daljinski pristup komponenti Internet Information Services (IIS)

# Pribavljanje sigurnosne zakrpe za Local Run Manager

Postoje četiri (4) mogućnosti pribavljanja sigurnosne zakrpe za Local Run Manager.

**1. mogućnost – preuzimanje izravno na instrument**

Najbrži način dolaska do sigurnosnog ažuriranja za Local Run Manager jest njegovo izravno preuzimanje na instrument s web-mjesta na kojem je hostirano.

1. Na instrument preuzmite alat za instalaciju zakrpe s veze navedene u sigurnoj poruci e-pošte.
2. Prenesite datoteku u mapu `C:\Illumina` na instrumentu.
3. Slijedite upute u odjeljku *Primjena sigurnosne zakrpe za Local Run Manager* na stranici 3.

**2. mogućnost – preuzimanje alata za instaliranje zakrpe na računalo i njegovo prebacivanje na instrument s pomoću USB pogona / dijeljene mape**

Ako ne možete preuzeti sigurnosnu zakrpu na instrument, preporučujemo da je preuzmete na zasebno računalo pa je prenesete na instrument.

Prije upotrebe potvrdite integritet USB pogona kod predstavnika za sigurnost (preporučuje se).

1. Preuzmite alat za instaliranje zakrpe s veze navedene u sigurnoj poruci e-pošte na stolno ili prijenosno računalo.
2. Preuzeti alat za instaliranje zakrpe kopirajte s računala na USB pogon ili u dijeljenu mapu.
3. U slučaju USB pogona, umetnite pogon u instrument.
4. Kopirajte alat za instaliranje zakrpe s USB pogona ili iz dijeljene mape u mapu `C:\Illumina` na instrumentu.
5. Slijedite upute u odjeljku *Primjena sigurnosne zakrpe za Local Run Manager* na stranici 3.

**3. mogućnost – traženje tehničke podrške**

Predstavnik službe za tehničku podršku tvrtke Illumina vodit će vas kroz postupak primjene zakrpe na neki od sljedećih načina:

- daljinska prijava tehničke podrške
  Predstavnik tehničke podrške daljinski će se prijaviti na analizator i instalirati zakrpu umjesto korisnika.

  Sustav treba biti daljinski dostupan. Ako imate pitanja, zatražite pomoć od lokalnog predstavnika IT odjela.

- vođenje kroz postupak
  Predstavnik tehničke podrške telefonski će vas voditi kroz postupak. Zatražite pomoć od lokalnog predstavnika službe za tehničku podršku.

**4. mogućnost – naručivanje unaprijed konfiguriranog pogona od tvrtke Illumina**

Korisnici mogu besplatno naručiti USB pogone zaštićene od pisanja. Da biste naručili pogon s instaliranom zakrpom, obratite se na adresu e-pošte techsupport@illumina.com.

Moguća su kašnjenja u slanju ili zastoji u skladištu koji mogu utjecati na vrijeme isporuke. Da biste sustave odmah zaštitili, toplo se preporučuje da se sustavi zaštite načinom koji će ponuditi najučinkovitiji put rješenja problema.

# Primjena alata za instalaciju sigurnosne zakrpe v.1.0 za Local Run Manager

Kad se pokrene Illumina MSI (Microsoft Installer), on će ažurirati konfiguraciju web-poslužitelja softvera Local Run Manager tako da se sprječava izvršavanje svih sadržaja koje su prenijeli korisnici i blokira sav daljinski pristup web-sučelju softvera Local Run Manager s LAN mreža.

Za korisnike koji upotrebljavaju web-sučelje softvera Local Run Manager za daljinski pristup instrumentima taj tijek rada nakon instalacije zakrpe više neće funkcionirati. Illumina namjerava kasnije vratiti tu funkcionalnost trajnim softverskim rješenjem tog problema. Ako to uzrokuje prekid ustaljenih tijekova rada, zatražite dodatnu pomoć putem adrese e-pošte techsupport@illumina.com.

Alat za instalaciju MSI funkcionira sa svim verzijama softvera Local Run Manager i automatski će odrediti konkretno rješenje na temelju verzije softvera Local Run Manager instalirane na instrumentu/računalu.

Taj će alat za instalaciju MSI stvoriti i datoteku revizije koja će uz vremensku oznaku pokazati da je ublažavanje posljedica primijenjeno kako bi se potvrdila pravilna instalacija.

Izvršavanje alata MSI Installer – pri prvom izvršavanju alata MSI Installer alat za instaliranje će zakrpati sustav i stvoriti datoteku revizije s vremenom završetka.

Ponovnim pokretanjem alata MSI Installer prikazat će se mogućnost **Repair** (Popravak) pa korisnik može ponovno primijeniti ili poništiti zakrpu. Napomena: poništavanjem zakrpe konfiguracija instrumenta postat će nesigurna.

# Primjena sigurnosne zakrpe za Local Run Manager

**Da biste instalirali zakrpu:**

1. Prijavite se u sustav s pomoću računa administratora (npr. sbsadmin).

Illumina preporučuje da se zakrpa primijeni kad instrument ne radi. Ako instrument izvodi obradu, zakrpu treba primijeniti netom nakon dovršetka obrade.

2. Pronađite zakrpu koja je preuzeta na sustav.
3. Premjestite alat za instaliranje zakrpe u mapu `C:\Illumina` (ona je isključena iz politike ograničenja za softver).
4. Dvokliknite ikonu alata za instaliranje da biste pokrenuli sučelje.
5. Kad se aplikacija učita, odaberite **Next** (Dalje) da biste započeli s instalacijom zakrpe.
6. Na zaslonu Installation Completion (Dovršetak instalacije) odaberite **Finish (Završi)**.

Ako je potrebna provjera izvješća o instalaciji, pogledajte odjeljak *Provjera valjanosti* na stranici 5.

Po završetku instalacije treba ponovno pokrenuti sustav.

**Popravak**

U slučaju pogreške korisnik može izvesti popravak instalacije praćenjem sljedećih uputa:

1. Prijavite se u sustav s pomoću računa administratora (npr. sbsadmin).
2. Pronađite zakrpu koja je preuzeta na sustav.
3. Premjestite alat za instaliranje zakrpe u mapu `C:\Illumina` (ona je isključena iz politike ograničenja za softver).
4. Dvokliknite ikonu alata za instaliranje da biste pokrenuli sučelje.
5. Alat za instaliranje automatski će prepoznati je li alat za konfiguraciju već izvođen i predstaviti nove mogućnosti:
   a. Change (Promijeni): zasivljeno i nije dostupno
   b. Repair (Popravi): popravlja pogreške i nudi mogućnosti ponovne konfiguracije.
   c. Remove (Ukloni): deinstalira zakrpu i vraća zadanu konfiguraciju (pogledajte odjeljak *Deinstalacija* na stranici 4)
6. Na zaslonu Installation Completion (Dovršetak instalacije) odaberite **Finish (Završi)**.

Ako je potrebna provjera izvješća o instalaciji, pogledajte odjeljak *Provjera valjanosti* na stranici 5.

Po završetku instalacije treba ponovno pokrenuti sustav.

**Deinstalacija**

Deinstalacijom zakrpe poništavaju se izmjene konfiguracijske datoteke na glavnom računalu aplikacije.

1. Prijavite se u sustav s pomoću računa administratora (npr. sbsadmin).
2. Pronađite zakrpu koja je preuzeta na sustav.
3. Premjestite alat za instaliranje zakrpe u mapu `C:\Illumina` (ona je isključena iz politike ograničenja za softver).
4. Dvokliknite ikonu alata za instaliranje da biste pokrenuli sučelje.
5. Odaberite **Remove (Ukloni)** da biste deinstalirali zakrpu i vratili sve vrijednosti na zadane postavke.

6. Odaberite **Remove (Ukloni)** da biste potvrdili mogućnost deinstalacije zakrpe i vraćanja svih vrijednosti na zadane postavke.

⚠ Ta će postavka učiniti sustav nesigurnim i podložnim napadu. Toplo se preporučuje prije odabira deinstalacije razmotriti sve tehničke utjecaje koje donosi mogućnost uklanjanja zakrpe.

7. Na zaslonu Installation Completion (Dovršetak instalacije) odaberite **Finish (Završi)**.

ℹ Ako je potrebna provjera izvješća o instalaciji, pogledajte odjeljak *Provjera valjanosti* na stranici 5.

ℹ Po završetku instalacije preporučuje se ponovno pokretanje sustava.

**Provjera valjanosti**

Ako postoji potreba za provjerom valjanosti instalacije, generira se datoteka s potvrdom valjanosti koja obuhvaća oznaku datuma i vremena, instaliranu verziju softvera Local Run Manager i druge vrijednosti ključne za provjeru valjanosti. Da biste dobili tu datoteku, obratite se na adresu e-pošte techsupport@illumina.com.

# Dodatne preporuke za ublažavanje posljedica i sigurnost

Sigurna implementacija RUO instrumenata i medicinskih uređaja Dx ovisi o razinama sigurnosti. Illumina toplo preporučuje da se instrumenti i uređaji implementiraju u najmanjoj podmreži ili sigurnosnom kontekstu zajedno s pouzdanim uređajima. Preporučuje se upotreba vatrozidova i drugih mrežnih politika za ograničavanje ulaznog i izlaznog pristupa.

Preporučujemo i sljedeće:

- Omogućite Transport Layer Security (TLS) da biste omogućili šifriranje sve komunikacije izvan instrumenta.
  - Da biste omogućili Transport Layer Security (TLS), pročitajte Priručnik za softver Local Run Manager.

# Zamjenske mogućnosti

Ako iz nekog razloga nije moguće izvršiti zakrpu, sljedeći načini ručnog ublažavanja posljedica mogu smanjiti rizik:

- Onemogućite daljinski pristup softveru Local Run Manager dodavanjem pravila za vatrozid sustava Windows kojima se blokiraju dolazna povezivanja na priključke 80 i 443.
  Alat MSI Installer automatski će blokirati daljinske dolazne veze u konfiguraciji web-poslužitelja softvera Local Run Manager. Ručno ublažavanje posljedica kojim se postiže isti rezultat jest implementacija konfiguracije vatrozida sustava Windows koja blokira dolazna `HTTP (TCP:80)` i `HTTPS (TLS, TCP:443)` povezivanja.

Kad se to implementira, softveru Local Run Manager može se pristupati isključivo s računala na kojemu je instaliran Local Run Manager; on više neće biti dostupan s drugih računala povezanih na istu mrežu.

Ako korisnikov tijek rada obuhvaća daljinski pristup softveru Local Run Manager, ta značajka više neće funkcionirati.

- Svedite broj drugih mrežnih uređaja na minimum.
  Ako konfigurirate mrežu tako da broj drugih mrežnih uređaja koji mogu komunicirati s odgovarajućim instrumentom svedete na minimum, smanjit ćete potencijal iskorištavanja ranjivosti. Što je manje veza dostupno u sustavu, to je manje mogućnosti za pristup.
  Za implementaciju toga možda ćete se morati posavjetovati s lokalnim stručnjakom za računalnu sigurnost ili informatičkim stručnjakom.
- Uklonite instrument s mreže.
  Ako nisu raspoložive druge mogućnosti, krajnja mjera za ublažavanje posljedica jest potpuno uklanjanje instrumenta s mreže. To će onemogućiti pristup uslugama Illumina Cloud/SaaS kao što su Proactive i BaseSpace® Sequence Hub te uobičajenim tijekovima rada koji obuhvaćaju prijenos genetičkih podataka.
  Za implementaciju toga možda ćete se morati posavjetovati s lokalnim stručnjakom za računalnu sigurnost ili informatičkim stručnjakom.

# Istraga mogućeg neovlaštenog pristupa

Sljedeći koraci mogu pomoći rukovatelju instrumenta da utvrdi je li sustavu pristupio neovlašteni korisnik:

1. Provjerite ima li u zapisnicima IIS-a pohranjenim u mapi `C:\inetpub\logs\LogFiles\W3SVC1` neuobičajenih poziva.
   - Uobičajeni pozivi web-poslužitelja softvera Local Run Manager izgledaju ovako:
     ```
     GET http /normalresource.extension?normal-URI-decoration
     ```
   - Mogu se, primjerice, pojaviti ovakvi neuobičajeni pozivi web-poslužitelja softvera Local Run Manager:
     ```
     POST http /hackertool.asp
     ```
2. U zapisniku IIS-a potražite tragove prijenosa sadržaja koji nisu datoteke manifesta putem metode POST. Primjerice, sljedeći pozivi upućivali bi na sumnjivu aktivnost:
   ```
   wscript
   shell
   wscript.network
   scripting.filesystemObject
   ```
3. Ako je instalirana aplikacija za zaštitu od virusa / zlonamjernog softvera, u zapisnicima softvera potražite znakove neuobičajenog ponašanja.

4. Provjerite ima li u zapisnicima sustava Windows tragova neuobičajenih poruka o pogreškama.
   Ako je zlonamjerni akter pristupio sustavu uz administratorske ovlasti, može mijenjati ili brisati sve lokalne zapisnike i događaje instrumenta.

Provjerite sve krajnje točke kojima je sustav mogao pokušati pristupiti. Popis očekivanih izlaznih veza potražite u odjeljku Vatrozid kontrolnog računala.

Ako je potrebno, zatražite pomoć od službe za tehničku podršku tvrtke Illumina.

# Povijest revizija

| Dokument | Datum | Opis promjene |
|---|---|---|
| Broj dokumenta 200017330 v02 | travanj 2022. | Dodana preporuka da se zakrpa primijeni kad instrument ne radi.<br>Dodana uputa o potrebi ponovnog pokretanja instrumenta nakon instalacije zakrpe.<br>Ispravljen opis povijesti revizija za v01. |
| Broj dokumenta 200017330 v01 | travanj 2022. | Promijenjen naslov dokumenta u Vodič s uputama za softversku zakrpu 1.0 za LRM.<br>Uklonjeno svako spominjanje verzije v1.0.1.<br>Dodan odjeljak posvećen istrazi mogućeg neovlaštenog pristupa. |
| Broj dokumenta 200017330 v00 | ožujak 2022. | Početno izdanje. |