Softverska zakrpa za LRM 1.0

illumina®

Vodič sa uputstvima

Uvod

Illumina® je upoznata sa bezbednosnom ranjivošću koja postoji u softveru Local Run Manager i obezbedila je softversku zakrpu za zaštitu od daljinske eksploatacije ove ranjivosti.

Local Run Manager je samostalna softverska aplikacija i deo podrazumevane konfiguracije sledećih sistema:

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

'Za in vitro dijagnostičku upotrebu.

Ovaj vodič važi za gorenavedene Illumina instrumente, kao i za i računare van instrumenata na kojima je instalirana samostalna verzija softvera Local Run Manager.

Ova ranjivost predstavlja neovlašćeno daljinsko izvršavanje komandi (Unauthenticated Remote Command Execution (RCE)) i ima CVSS ocenu nerešavanja 10.0 tj. kritičnu: `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H`.

Sledeći koraci za suzbijanje rizika obavezni su na svim platformama da biste se osigurali od mogućnosti da nosilac pretnje dobije pristup nekim instrumentima i izvrši napad nakon daljinskog pristupa.

Ukoliko instalacioni program ne može da se pokrene iz nekog razloga, uzmite u obzir odeljak sa dodatnim merama za suzbijanje rizika pri kraju ovog dokumenta ili se obratite na adresu techsupport@illumina.com da biste dobili dodatnu pomoć.

Pogledajte odeljak Pribavljanje ispravki za Local Run Manager da biste pronašli opcije kako da preuzmete ili zatražite kopiju zakrpe.

- **Zakrpa v1.0.0** će ažurirati veb-konfiguraciju softvera Local Run Manager i onemogućiti daljinski pristup preko Internet Information Services (IIS) usluga.

Pribavljanje bezbednosne zakrpe za Local Run Manager

Postoji četiri (4) načina da pribavite bezbednosnu zakrpu za Local Run Manager.

Opcija 1 – Preuzimanje direktno na instrument

Najbrži način da pribavite bezbednosnu ispravku za Local Run Manager jeste da je preuzmete sa veb-sajta hosta direktno na instrument.

1. Preuzmite instalacioni program zakrpe preko veze koja je navedena u bezbednoj e-poruci na svoj instrument.
2. Prenesite datoteku u fasciklu `C:\Illumina` na instrumentu.
3. Pratite uputstva iz odeljka *Primena bezbednosne zakrpe za Local Run Manager* na strani 4.

Opcija 2 – Preuzimanje instalacionog programa zakrpe i prenos na instrument preko USB diska/deljene fascikle

Ako ne možete da preuzmete bezbednosnu zarpu na instrument, preporučujemo da je preuzmete na drugi računar, a zatim prenesete na instrument.

Pre upotrebe, potvrdite integritet USB diska kod svojih predstavnika za bezbednost. (Preporučuje se)

1. Preuzmite instalacioni program zakrpe preko veze koja je navedena u bezbednoj e-poruci na svoj računar ili laptop.
2. Kopirajte preuzeti instalacioni program zakrpe sa računara na USB disk ili u deljenu fasciklu.
3. Ako koristite USB disk, priključite disk na instrument.
4. Kopirajte preuzeti instalacioni program zakrpe sa USB diska ili iz deljene fascikle u fasciklu `C:\Illumina` na instrumentu.
5. Pratite uputstva iz odeljka *Primena bezbednosne zakrpe za Local Run Manager* na strani 4.

Opcija 3 – Zahtevanje tehničke podrške

Predstavnik tehničke podrške kompanije Illumina će vas provesti kroz proces primene zakrpe korišćenjem jedne od ovih metoda:

- Daljinska prijava iz tehničke podrške
  Predstavnik tehničke podrške daljinski pristupiti analizatoru i instaliraće zakrpu za korisnika.

  Sistem će morati da ima mogućnost daljinskog pristupa. Ako imate bilo kakva pitanja, obratite se lokalnom IT predstavniku za pomoć.

- Navođena uputstva
  Predstavnik tehničke podrške će pružiti navođena uputstva putem telefona. Obratite se svom lokalnom predstavniku tehničke podrške za pomoć.

Opcija 4 – Naručivanje unapred konfigurisanog diska od kompanije Illumina

Korisnici mogu da naruče USB diskove koji su zaštićeni od upisivanja bez naknade. Da biste naručili disk sa instaliranom zakrpom, obratite se na adresu techsupport@illumina.com.

Mogli bi se javiti zastoji u isporuci ili sa zalihama koji utiču na vremenske rokove dostave. Da bi se sistemi što pre zaštitili, izričito se preporučuje da se za njihovu zaštitu koristi onaj metod koji nudi najefikasniji put rešavanja problema.

Primena instalacionog programa bezbednosne zakrpe za Local Run Manager Patch v.1.0

Illumina MSI (Microsoft instalacioni program) će, nakon izvršavanja, ažurirati konfiguraciju veb servera za Local Run Manager da bi sprečio izvršavanje svakog korisnički otpremljenog sadržaja i blokirao sav pristup veb-interfejsu modula Local Run Manager preko LAN mrežnih veza.

Kod onih korisnika koji daljinski pristupaju instrumentima preko veb-interfejsa modula Local Run Manager, ovaj tok rada će prestati da funkcioniše nakon instalacije ove zakrpe. Illumina namerava da kasnije vrati ovu funkcionalnost trajnom softverskom popravkom ovog problema. Ako ovo dovede do prekida u uspostavljenim tokovima rada, obratite se na adresu techsupport@illumina.com da biste dobili dodatnu pomoć.

Instalacioni program MSI može se primeniti na sve verzije modula Local Run Manager i on će automatski odrediti dobru popravku na osnovu verzije modula Local Run Manager koja je instalirana na instrumentu/računaru.

Ovaj instalacioni program MSI će takođe napraviti datoteku revizije koja pokazuje da je ovo suzbijanje rizika sprovedeno i sadrži vremensku oznaku koja će pokazivati adekvatnu instalaciju.

Pokretanje instalacionog programa MSI – kada prvi put pokrenete instalacioni program MSI, on će zakrpiti sistem i napraviti datoteku revizije sa vremenom završetka.

Ponovno pokretanje instalacionog programa MSI će predstaviti opciju **Repair** (Popravi) i korisnik će dobiti opciju da ponovo primeni ili poništi zakrpu. Napomena: poništavanje zakrpe će dovesti do nebezbedne konfiguracije instrumenta.

Primena bezbednosne zakrpe za Local Run Manager

Da biste instalirali zakrpu:

1. Prijavite se na sistem putem administratorskog naloga (npr. sbsadmin).

   Illumina preporučuje primenu zakrpe dok instrument ne radi. Ako se na instrumentu izvršava neka obrada, zakrpu treba primeniti čim se obrada završi.

2. Pronađite zakrpu koja je preuzeta na sistem.
3. Premestite instalacioni program zakrpe u fasciklu `C:\Illumina` (sa izuzećem od smernica za restrikciju softvera).
4. Kliknite dvaput na ikonu instalacionog programa da biste pokrenuli interfejs.
5. Kada se aplikacija učita, izaberite dugme **Next** (Dalje) da biste započeli instalaciju zakrpe.
6. Na ekranu Installation Completion (Završetak instalacije) izaberite opciju **Finish** (Završi).

U slučaju da je verifikacija izveštaja o instalaciji neophodna, pogledajte odeljak *Verifikacija* na strani 5.

Ponovno pokretanje sistema nakon instalacije je obavezno.

Popravka

U slučaju greške, korisnik može da izvrši popravku instalacije prateći ova uputstva:

1. Prijavite se na sistem putem administratorskog naloga (npr. sbsadmin).
2. Pronađite zakrpu koja je preuzeta na sistem.
3. Premestite instalacioni program zakrpe u fasciklu `C:\Illumina` (sa izuzećem od smernica za restrikciju softvera).
4. Kliknite dvaput na ikonu instalacionog programa da biste pokrenuli interfejs.
5. Instalacioni program će automatski otkriti da li je alatka za konfiguracija ranije bila izvršavana i ponudiće nove opcije:
   a. Change (Promeni): zatamnjena i nedostupna
   b. Repair (Popravi): popravlja greške i nudi opcije za promenu konfiguracije.
   c. Remove (Ukloni): deinstalira zakrpu i vraća je na podrazumevanu konfiguraciju (pogledajte odeljak *Deinstalacija* na strani 5)
6. Na ekranu Installation Completion (Završetak instalacije) izaberite opciju **Finish** (Završi).

U slučaju da je verifikacija izveštaja o instalaciji neophodna, pogledajte odeljak *Verifikacija* na strani 5.

Ponovno pokretanje sistema nakon instalacije je obavezno.

Deinstalacija

Deinstalacija zakrpe poništava izmene koje su unete u datoteku konfiguracije hosta aplikacije.

1. Prijavite se na sistem putem administratorskog naloga (npr. sbsadmin).
2. Pronađite zakrpu koja je preuzeta na sistem.
3. Premestite instalacioni program zakrpe u fasciklu `C:\Illumina` (sa izuzećem od smernica za restrikciju softvera).
4. Kliknite dvaput na ikonu instalacionog programa da biste pokrenuli interfejs.
5. Izaberite opciju **Remove** (Ukloni) da biste deinstalirali zakrpu i vratili sve vrednosti na podrazumevana podešavanja.
6. Izaberite opciju **Remove** (Ukloni) da biste verifikovali opciju za deinstaliranje zakrpe i vratili sve vrednosti na podrazumevana podešavanja.

⚠ Ovo podešavanje će dovesti do nebezbednog sistema koji je u riziku od napada. Izričito se preporučuje da se svi tehnički uticaji koji dovode do opcije za uklanjanje zakrpe otklone pre nego što odaberete deinstalaciju.

7. Na ekranu Installation Completion (Završetak instalacije) izaberite opciju **Finish** (Završi).

ℹ U slučaju da je verifikacija izveštaja o instalaciji neophodna, pogledajte odeljak *Verifikacija* na strani 5.

ℹ Preporučuje se ponovno pokretanje sistema nakon instalacije.

Verifikacija

Ako postoji potreba da se instalacija verifikuje, biće generisana datoteka za verifikaciju koja sadrži oznaku datuma i vremena, verziju instaliranog softvera Local Run Manager i druge ključne vrednosti za verifikaciju. Da biste nabavili ovu datoteku, obratite se na adresu techsupport@illumina.com.

Dodatne preporuke za suzbijanje rizika i bezbednost

Bezbedna primena RUO instrumenata i Dx medicinskih sredstava zavisi od slojeva zaštite. Illumina izričito preporučuje da se svi instrumenti i uređaji primenjuju u najmanjoj podmreži ili bezbednosnom kontekstu mreže u kojima su ostali pouzdani uređaji. Izrazito se preporučuje korišćenje zaštitnog zida i drugih mrežnih smernica za ograničavanje ostalog dolaznog i odlaznog pristupa.

Takođe preporučujemo:

- Omogućite protokol Transport Layer Security (TLS) da biste osigurali šifrovanje svake komunikacije koja teče preko instrumenta.
  - Da biste omogućili Transport Layer Security (TLS), pogledajte Vodič za softver Local Run Manager.

Alternativne opcije

Ako izvršavanje zakrpe nije izvodljivo iz nekog razloga, sledeće ručne metode za suzbijanje rizika će smanjiti rizik:

- Onemogućite daljinski pristup modulu Local Run Manager dodavanjem pravila za Windows zaštitni zid koja će blokirati veze sa portovima 80 i 443.
  Instalacioni program MSI automatski će blokirati daljinske dolazne veze u okviru konfiguracije veb servera za Local Run Manager. Ručno suzbijanje rizika kojim se postiže isti rezultat sastoji se od primene konfiguracije za Windows zaštitni zid koja će blokirati dolazne veze ka portovima `HTTP (TCP:80)` i `HTTPS (TLS, TCP:443)`.
  Kada se implementira, modulu Local Run Manager može da se pristupa samo na računaru na kom je Local Run Manager instaliran; više neće moći da mu se pristupa sa drugih računara koji su povezani na istu mrežu.

Ako korisnički tok rada uključuje daljinski pristup modulu Local Run Manager, ova funkcionalnost više neće raditi.

- Svedite broj ostalih uređaja u mreži na minimum.
  Konfigurisanje mreže tako da se broj ostalih uređaja u mreži koji mogu da komuniciraju sa zahvaćenim instrumentom svede na minimum će smanjiti potencijal za eksploataciju. Što je manje veza dostupno sistemu, manje je raspoloživih prilika za pristup.
  Možda ćete morati da se konsultujete sa odeljenjem lokalne informatičke bezbednosti ili IT resursa da biste ovo sproveli.
- Sklonite instrument sa mreže.
  Ako nijedna druga opcija nije izvodljiva, poslednja mera suzbijanja rizika je da sklonite instrument sa mreže. Ovo će onemogućiti pristup Illumina uslugama u oblaku/SaaS uslugama, kao što su Proactive i BaseSpace® Sequence Hub, kao i tipičnim radnim tokovima sa skidanjem podataka o genomima.
  Možda ćete morati da se konsultujete sa odeljenjem lokalne informatičke bezbednosti ili IT resursa da biste ovo sproveli.

Istraga potencijalnog neovlašćenog pristupa

Sledeći koraci mogu biti od pomoći operateru instrumenta da utvrdi da li je neki neovlašćeni korisnik pristupao sistemu:

1. Ispitivanje da li IIS evidencije koje se čuvaju u datoteci `C:\inetpub\logs\LogFiles\W3SVC1` sadrže abnormalne pozive.

- Normalni pozivi upućeni veb-serveru za Local Run Manager izgledaju ovako:

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

- Abnormalni pozivi upućeni veb-serveru za Local Run Manager mogli bi, na primer, da izgledaju ovako:

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

2. Ispitivanje da li IIS evidencija sadrži znake POST otpremanja ili sadržaja koji ne čine datoteke manifesta. Na primer, sledeći pozivi bi ukazivali na sumnjive aktivnosti:

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

3. Ako je instalirana neka antivirusna/antimalver aplikacija, proverite da li u evidenciji softvera postoje znaci abnormalnog ponašanja.
4. Ispitajte da li u Windows datotekama evidencije postoje znaci abnormalnih poruka o greškama.
   Ako je neki preteći akter ostvario pristup uz prava administratora, imaće mogućnost da izmeni ili izbriše sve lokalne evidencije i događaje sa instrumenta.

Proverite da li je sistem možda isprobavao pristup bilo kakvim krajnjim tačkama. Za listu očekivanih odlaznih veza pogledajte Zaštitni zid kontrolnog računara.

Obratite se tehničkoj podršci kompanije Illumina za pomoć po potrebi.

Istorija revizija

Dokument	Datum	Opis promene
Br. dokumenta 200017330 v02	April 2022.	Dodata je preporuka da se zakrpa primeni dok instrument ne radi. Dodato je uputstvo za obavezno ponovno pokretanje instrumenta nakon instalacije zakrpe. Ispravljen je opis istorije revizija za v01.
Br. dokumenta 200017330 v01	April 2022.	Naslov dokumenta je promenjen u Vodič sa uputstvima za softversku zakrpu za LRM 1.0 Uklonjeno je svako pominjanje v1.0.1. Dodat je odeljak koji pokriva istragu potencijalnog neovlašćenog pristupa.
Br. dokumenta 200017330 v00	Mart 2022.	Početno izdanje.