

Kasutusjuhend

Sissejuhatus

illumina® on saanud teada tarkvaras Local Run Manager olevast turvaaugust ja pakkunud tarkvarapaiga, mis kaitseb selle haavatavuse kaugkasutamise eest.

Local Run Manager on eraldiseisev tarkvararakendus, mis on järgmiste süsteemide vaikekonfiguratsiooni osa:

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

*In vitro diagnostiliseks kasutamiseks.

See juhend kehtib eespool loetletud illumina instrumentide ja seadmeväliste arvutite kohta, millesse on installitud tarkvara Local Run Manager eraldiseisev versioon.

Turbenõrkus on autentimata kaugkäskäitus (Unauthenticated Remote Command Execution, RCE) täieliku CVSS-i skooriga 10,0 ehk kriitiline, CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H.

Järgmisi riskivähenduse meetmeid tuleb kasutada eespool loetletud instrumentidel, et tagada ühele või mitmele seadmele kaitse võimaliku volitamata kasutaja juurdepääsu ja kaugjuurdepääsu kaudu tehtava rünnaku eest.

Kui mingil põhjusel pole võimalik installerit kasutada, tutvuge selle dokumendi lõpus toodud täiendavate riskivähenduse meetmetega või võtke lisaabi saamiseks ühendust tehnilise toega aadressil techsupport@illumina.com.

Paiga allalaadimise või taotlemise võimalusi vt jaotisest [Tarkvara Local Run Manager värskenduse hankimine](#).

- **Paik v1.0.0** – värskendab tarkvara Local Run Manager veebikonfiguratsiooni ja keelab interneti andmeteenuste (Internet Information Services, IIS) kaugjuurdepääsu.

Tarkvara Local Run Manager turbepaiga hankimine

Tarkvara Local Run Manager turbepaiga hankimiseks on neli (4) võimalust.

1. võimalus – otse seadmesse allalaadimine

Kiireim viis tarkvara Local Run Manager turbevärskenduse hankimiseks on see majutusveebilehelt otse seadmesse alla laadida.

1. Laadige paiga installer turvalise meili kaudu saadud lingilt oma seadmesse alla.
2. Teisaldage fail seadmes kausta C:\Illumina.
3. Järgige jaotises [Tarkvara Local Run Manager turbepaiga kasutamine leheküljel 3](#) toodud juhiseid.

2. võimalus – paiga installeri arvutisse allalaadimine ja USB-ketta / jagatud kausta abil seadmesse viimine

i | Kui te ei saa seadmesse turvapaika alla laadida, soovitame selle alla laadida eraldi arvutisse ja seejärel seadmesse üle kanda.

Enne kasutamist kontrollige USB-ketta terviklikkust turbespetsialistide abil. (Soovitatav)

1. Laadige paiga installer turvalise meili kaudu saadud lingilt oma arvutisse või sülearvutisse alla.
2. Kopeerige allalaaditud paiga installer arvutist USB-kettale või jagatud kausta.
3. USB-kettale kopeerimiseks ühendage ketas seadmega.
4. Kopeerige paiga installer USB-kettalt või jagatud kaustast seadme kausta C:\Illumina.
5. Järgige jaotises [Tarkvara Local Run Manager turbepaiga kasutamine leheküljel 3](#) toodud juhiseid.

3. võimalus – tehnilise toe tellimine

Illumina tehnilise toe esindaja juhendab teid paikamise käigus ühega järgmistest meetoditest.

• Tehnilise toe kaugsisselõigimine

Tehnilise toe esindaja siseneb kaugühenduse kaudu analüsaatorisse ja installib paiga kliendi eest.

i | Selleks peab süsteemile olema kaugjuurdepääs. Küsimuste tekkimisel paluge abi kohalikul IT-spetsialistilt.

• Juhendamine

Tehnilise toe esindaja juhendab teid telefoni teel. Võtke abi saamiseks ühendust tehnilise toe kohaliku esindajaga.

4. võimalus – ettevõttelt Illumina eelkonfigureeritud ketta tellimine

Kliendid saavad tellida tasuta kirjutuskaitstud USB-ketta. Installitud paigaga ketta tellimiseks võtke ühendust tehnilise toega aadressil techsupport@illumina.com.

i | Saadetise õigeaegset kohaletoometamist võivad mõjutada hilinemised tarnetes või inventar. Süsteemide kiiremaks kaitsmiseks on väga soovitatav kasutada kõige tõhusama lahendusteege meetodit.

Tarkvara Local Run Manager turbepaiga v.1.0 installeri kasutamine

Kui kasutate Illumina MSI-d (Microsoft Installerit), parandab see tarkvara Local Run Manager veebiserveri konfiguratsiooni, et ennetada mis tahes kasutaja üles laaditud sisu kasutamist ja blokeerida kogu kaugjuurdepääs tarkvara Local Run Manager veebiliidesele LAN-võrguühenduste kaudu.

i | Kasutajatel, kes kasutavad tarkvara Local Run Manager veebiliidest seadmetele kaugjuurdepääsuks, lõpetab taoline töövoog pärast selle paiga installimist toimimise. Illumina taastab edaspidi selle funktsiooni tarkvaraprobleemi püsiparandusega. Kui meetme kasutamisest tekib paika pandud töövoogude katkestus, võtke tehnilise abi saamiseks ühendust aadressil techsupport@illumina.com.

MSI Installer toimib kõikide tarkvara Local Run Manager versioonidega ja tuvastab automaatselt õige paranduse vastavalt seadmesse/arvutisse installitud tarkvara Local Run Manager versioonile.

MSI Installer loob ka auditifaili, milles näidatakse kasutatud riskivähenduse meetet koos asjakohase installimise ajatempliga.

MSI Installeri käitamine – MSI Installeri esmakordsel käitamisel paikab installer süsteemi ja loob auditifaili lõpetamise ajaga.

i | MSI Installeri uuesti käitamisel pakutakse suvandit **Repair** (Paranda), millega kasutaja saab paiga uuesti installida või tagasi pöörata. Märkus. Paiga tagasi pööramine põhjustab seadme konfiguratsiooni ebaturvalisust.

Tarkvara Local Run Manager turbepaiga kasutamine

Paiga installimiseks tehke järgmist.

1. Logige süsteemi sisse administraatorikontoga (nt sbsadmin).

i | Illumina soovib paiga rakendada siis, kui seade ei tööta. Kui seadet käitatakse, tuleb paik rakendada kohe pärast käitamise lõppu.

2. Leidke süsteemi allalaaditud paik.

3. Teisaldage paiga installer kausta C:\Illumina (vabastatud tarkvara piirangupoliitikast).

4. Liidese käivitamiseks topeltklõpsake installeri ikoonil.
5. Pärast rakenduse laadimist valige nupp **Next** (Järgmine), et alustada paiga installimist.
6. Valige installimise lõpukuval nupp **Finish** (Valmis).

i | Juhul kui vajate installimise aruande kinnitamist, vt jaotist [Kinnitamine leheküljel 5](#).

i | Installimise lõpus tuleb süsteem taaskäivitada.

Parandamine

Vea tekkimisel saab klient installi parandada, järgides allolevaid juhiseid.

1. Logige süsteemi sisse administraatorikontoga (nt sbsadmin).
2. Leidke süsteemi allalaaditud paik.
3. Teisaldage paiga installer kausta C:\Illumina (vabastatud tarkvara piirangupoliitikast).
4. Liidese käivitamiseks topeltklõpsake installeri ikoonil.
5. Installer tuvastab automaatselt, kas konfigureerimistööriista on varem kasutatud, ja pakub välja uued valikud.
 - a. Change (Muuda): hall ja pole kättesaadav.
 - b. Repair (Paranda): parandab vead ja pakub uuesti konfigureerimise valikut.
 - c. Remove (Eemalda): desinstallib paiga ja taastab vaikekonfiguratsiooni (vt jaotist [Desinstallimine leheküljel 4](#)).
6. Valige installimise lõpukuval nupp **Finish** (Valmis).

i | Juhul kui vajate installimise aruande kinnitamist, vt jaotist [Kinnitamine leheküljel 5](#).

i | Installimise lõpus tuleb süsteem taaskäivitada.

Desinstallimine

Paiga desinstallimine pöörab tagasi rakenduse hosti konfiguratsioonifailis tehtud muudatused.

1. Logige süsteemi sisse administraatorikontoga (nt sbsadmin).
2. Leidke süsteemi allalaaditud paik.
3. Teisaldage paiga installer kausta C:\Illumina (vabastatud tarkvara piirangupoliitikast).
4. Liidese käivitamiseks topeltklõpsake installeri ikoonil.
5. Valige nupp **Remove** (Eemalda) paiga desinstallimiseks ja kõigi väärtuste vaikesätete taastamiseks.
6. Valige nupp **Remove** (Eemalda), et kinnitada valikut paiga desinstallimiseks ja kõigi väärtuste vaikesätete taastamiseks.

! | Taoline seadistus muudab süsteemi ebatavaliseks ja tekitab rünnaku ohu. Enne desinstallimise otsustamist on väga soovitatav kaaluda mis tahes tehnilisi mõjutegureid, mis tingivad paiga eemaldamise valiku kasutamist.

7. Valige installimise lõpukuval nupp **Finish** (Valmis).

i | Juhul kui vajate installimise aruande kinnitamist, vt jaotist [Kinnitamine leheküljel 5](#).

i | Installimise lõpus on soovitatav teha süsteemile taaskäivitus.

Kinnitamine

Kui tekib vajadus installimist kinnitada, siis on selleks loodud kinnitusfail, mis sisaldab kuupäeva ja ajatemplit, installitud tarkvara Local Run Manager versiooni ja teisi olulisi kinnitamisväärtusi. Selle faili saamiseks võtke ühendust tehnilise toega aadressil techsupport@illumina.com.

Täiendavad riskivähenduse ja turbesoovitused

RUO instrumentide ja Dx-mediitsiiniseadmete turvaline kasutuselevõtt sõltub turbekihtidest. Ettevõtte Illumina tungival soovitusel tuleks seadmeid kasutada võrgu väikseimas alamvõrgus või turbekontekstis koos usaldusväärsete seadmetega. Väga soovitatav on kasutada tulemüüre ja teisi võrgupoliitikaid, mis piiravad muud sissetulevat ja väljaminevat juurdepääsu.

Soovitame ka järgmist.

- Lubage transpordikihi turbeprotokoll (Transport Layer Security, TLS) veendumaks, et kogu seadmeteväline andmeside oleks krüpteeritud.
 - Transpordikihi turbeprotokolli (TLS) lubamise kohta lugege tarkvara Local Run Manager juhendist.

Alternatiivsed meetmed

Kui paika ei ole mingil põhjusel võimalik kasutada, saab riski vähendada järgmiste manuaalsete meetoditega.

- Keelake tarkvara Local Run Manager kaugjuurdepääs, lisades Windowsi tulemüürireeglid, mis blokeerivad portide nr 80 ja 443 sissetulevad ühendused.

Rakendus MSI Installer blokeerib automaatselt sissetulevad kaugühendused tarkvara Local Run Manager veebiserveri konfiguratsioonis. Sama tulemust on võimalik saavutada, kui sisestate käsitsi Windowsi tulemüüri konfiguratsiooni, mis blokeerib HTTP (TCP:80) ja HTTPS-i (TLS, TCP:443) sissetulevad ühendused.

Pärast nende meetmete võtmist pääseb tarkvarale Local Run Manager ligi ainult selles arvutis, millesse Local Run Manager on installitud; teistel samasse võrku ühendatud arvutitel puudub juurdepääs tarkvarale.

i | Kui kasutaja töövoog hõlmab kaugjuurdepääsu tarkvarale Local Run Manager, siis see funktsioon enam ei toimi.

- Vähendage teiste võrguseadmete arvu.

Võrgu konfigureerimine nii, et võimalikult vähestel võrguseadmetel oleks sideühendus mõjutatud seadmega, vähendab nõrkuse ärakasutamise võimalust. Mida vähem on süsteemis ühendusi, seda väiksem on juurdepääsu võimalus.

Selleks võib vaja minna konsulteerimist kohalike andmeturbe või IT-spetsialistidega.

- Eemaldage seade võrgust.

Kui muid võimalusi ei saa kasutada, on viimane riskivähenduse meede eemaldada seade täielikult võrgust.

Sellega blokeeritakse juurdepääs teenustele Illumina Cloud/SaaS, nagu Proactive ja BaseSpace® Sequence Hub, ning tüüpilistele genoomiandmete allalaadimisega töövoogudele.

Selleks võib vaja minna konsulteerimist kohalike andmeturbe või IT-spetsialistidega.

Võimaliku volitamata juurdepääsu uurimine

Järgmised toimingud võivad aidata seadme operaatoril kindlaks teha, kas volitamata kasutaja on süsteemile juurde pääsenud.

1. Kontrollige IIS-i logisid kaustas `C:\inetpub\logs\LogFiles\W3SVC1` ebatavaliste kõnede suhtes.

- Tavapärased kõned tarkvara Local Run Manager veebiserverisse näevad välja järgmised:

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

- Ebatavalised kõned tarkvara Local Run Manager veebiserverisse võivad välja näha näiteks järgmised.

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

2. Kontrollige IIS-i logi manifestifailidest erineva sisu POST-üleslaadimiste suhtes. Näiteks viitavad järgmised kõned kahtlasele tegevusele:

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

3. Kui installitud on viiruse-/ründevaratõrje rakendus, kontrollige tarkvaralogisid ebatavalise käitumise märkide suhtes.
4. Kontrollige Windowsi logisid ebatavaliste tõrketeadete suhtes.
Kui ohutegur sai administraatoriõigustega juurdepääsu, saab ta muuta või kustutada kõiki kohalikke seadmelogisid ja sündmusi.

Kontrollige kõiki lõpp-punkte, millele süsteem võib olla üritanud juurde pääseda. Oodatavate väljaminevate ühenduste loendit vaadake lehelt [Juhtarvuti tulemüür](#).

Kui vajate abi, pöörduge Illumina tehnilise toe poole.

Muudatuste ajalugu

Dokument	Kuupäev	Muudatuse kirjeldus
Dokument nr 200017330 v02	Aprill 2022	Lisati soovitus paiga rakendamise kohta, kui seade ei tööta. Lisati juhised, mille kohaselt on pärast paiga installimist tarvis seade taaskäivitada. Parandati versiooni 01 redaktsioonijaloo kirjeldust.
Dokument nr 200017330 v01	Aprill 2022	Dokumendi uus pealkiri on „Tarkvara LRM paiga 1.0 kasutusjuhend“. Eemaldati kõik viited versioonile v1.0.1. Lisati jaotis, mis hõlmab võimaliku volitamata juurdepääsu uurimist.
Dokument nr 200017330 v00	Märts 2022	Algversioon.

See dokument ja selle sisu kuuluvad ettevõttele Illumina, Inc. ja selle tütarettevõtetele („Illumina“) ning on mõeldud kasutamiseks ainult ettevõtte lepingulistele klientidele seoses selles dokumendis kirjeldatud toote (toodete) kasutamisega ega ole mõeldud mitte mingiks muuks otstarbeks. Seda dokumenti ega selle sisu ei tohi mis tahes viisil kasutada ega muul eesmärgil levitada ja/või edastada, avaldada või reprodutseerida ilma Illumina eelneva kirjaliku nõusolekuta. Illumina ei anna selle dokumendiga kolmandale isikule oma patendi-, kaubamärgi-, autori-, tava- või muu sarnase õiguse alusel mitte ühtegi litsentsi.

Kvalifitseeritud ja asjakohase koolituse saanud töötajad peavad selles dokumendis kirjeldatud juhiseid järgima rangelt ja üksikasjalikult, et tagada siin kirjeldatud toote (toodete) õige ja ohutu kasutusviis. Siinse dokumendi sisu tuleb enne nimetatud toote (toodete) kasutamist täies ulatuses läbi lugeda ja endale selgeks teha.

SELLES DOKUMENDIS KIRJELDATUD JUHISTE MITTE LUGEMINE JA MITTE ÜKSİKASJALIKULT JÄRGIMINE VÕIB KAHJUSTADA TOODET (TOOTEID), VIGASTADA INIMESI (SH KASUTAJAID VÕI TEISI) JA KAHJUSTADA MUUD VARA. NIMETATUD JUHUL EI KEHTI ÜKSKI TOOTELE (TOODETELE) ANTUD GARANTII.

ILLUMINA EI VASTUTA SELLES DOKUMENDIS KIRJELDATUD TOOTE (TOODETE) (SEALHULGAS TOOTE OSAD VÕI TARKVARA) VÄÄRKASUTUSE EEST.

© 2022 Illumina, Inc. Kõik õigused kaitstud.

Kõik kaubamärgid kuuluvad ettevõttele Illumina, Inc. või nende vastavatele omanikele. Teavet konkreetsete kaubamärkide kohta vaadake veebilehelt www.illumina.com/company/legal.html.