LRM programinės įrangos 1.0 pataisa

illumina®

Instrukcijų vadovas

Įvadas

„Illumina®“ sužinojo apie „Local Run Manager“ programinės įrangos saugos pažeidžiamumą ir pateikė programinės įrangos pataisą, apsaugančią nuo nuotolinio pažeidžiamumo išnaudojimo.

„Local Run Manager“ yra atskira programa, įtraukta į numatytąją konfigūraciją šiose sistemose:

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

* Naudoti in vitro diagnostikai.

Šis vadovas taikomas pirmiau nurodytiems „Illumina“ instrumentams ir neinstrumentiniams kompiuteriams, kuriuose įdiegta atskira „Local Run Manager“ versija.

Pažeidžiamumas – tai neautentifikuotas nuotolinis komandų vykdymas, kurio CVSS įvertis nesiėmus rizikos mažinimo priemonių yra 10.0, kritinis, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H`.

Pirmiau nurodytuose instrumentuose reikia atlikti toliau nurodytus rizikos mažinimo veiksmus, siekiant apsisaugoti nuo galimybės, kad neteisėtas naudotojas pasieks vieną ar daugiau instrumentų ir įvykdys nuotolinį išpuolį.

Jei dėl kokios nors priežasties diegimo programos negalima paleisti, skaitykite šio dokumento pabaigoje esantį skyrių apie papildomus rizikos mažinimo būdus arba susisiekite adresu techsupport@illumina.com, kad gautumėte papildomos pagalbos.

Žr. skiltį „Local Run Manager“ naujinimo gavimas, jei norite sužinoti, kaip atsisiųsti pataisą arba paprašyti jos kopijos.

- **v1.0.0 pataisa** atnaujins „Local Run Manager“ žiniatinklio konfigūraciją ir išjungs nuotolinę interneto informacijos tarnybų (IIS) prieigą.

Naudoti tik moksliniams tyrimams. Negalima naudoti atliekant diagnostikos procedūras.

„Local Run Manager“ saugos pataisos gavimas

Yra keturi (4) „Local Run Manager“ saugos pataisos gavimo būdai.

1 būdas. Atsisiuntimas į jūsų instrumentą

Greičiausias būdas gauti „Local Run Manager“ saugos naujinimą – atsisiųsti jį tiesiai iš prieglobos svetainės į instrumentą.

1. Atsisiųskite pataisos diegimo programą iš saugiu el. paštu pateiktos nuorodos į savo instrumentą.
2. Perkelkite failą į instrumento aplanką `C:\Illumina`.
3. Vadovaukitės nurodymais skyriuje *„Local Run Manager“ saugos pataisos taikymas* 4 psl..

2 būdas. Pataisos diegimo programos atsisiuntimas į kompiuterį ir perkėlimas į instrumentą naudojant USB atmintinę / bendrinamą aplanką

Jei negalite atsisiųsti instrumento saugos pataisos, rekomenduojame ją atsisiųsti į atskirą kompiuterį ir perkelti į instrumentą.

Prieš naudodami USB atmintinę, kartu su savo saugos atstovais patikrinkite jos vientisumą. (Rekomenduojama)

1. Atsisiųskite pataisos diegimo programą iš saugiu el. paštu pateiktos nuorodos į savo stacionarų ar nešiojamąjį kompiuterį.
2. Nukopijuokite atsisiųstą pataisos diegimo programą į USB atmintinę arba kompiuterio bendrinamą aplanką.
3. Jei naudojate USB atmintinę, prijunkite ją prie instrumento.
4. Nukopijuokite pataisos diegimo programą iš USB atmintinės arba bendrinamo aplanko į `C:\Illumina` aplanką instrumente.
5. Vadovaukitės nurodymais skyriuje *„Local Run Manager“ saugos pataisos taikymas* 4 psl..

3 būdas. Techninės pagalbos prašymas

„Illumina“ techninės pagalbos atstovas padės jums atlikti pataisos diegimo procesą vienu iš toliau nurodytų būdų.

- Techninės pagalbos nuotolinis prisijungimas
  Techninės pagalbos atstovas nuotoliniu būdu prisijungs prie analizatoriaus ir kliento vardu įdiegs pataisą.

  Sistema turi būti pasiekiama nuotoliniu būdu. Jei turite klausimų, kreipkitės pagalbos į vietinį IT atstovą.

- Instrukcijos
  Techninės pagalbos atstovas teiks nurodymus telefonu. Dėl pagalbos kreipkitės į vietinį techninės pagalbos atstovą.

4 būdas. Užsisakykite iš anksto sukonfigūruotą atmintinę iš „Illumina“

Apsaugotas nuo įrašymo USB atmintines klientas gali užsisakyti nemokamai. Norėdami užsisakyti atmintinę su įdiegta pataisa, susisiekite adresu techsupport@illumina.com.

Siuntos ar atsargos gali vėluoti, tai gali turėti įtakos pristatymo laikui. Jei norite nedelsiant apsaugoti sistemas, labai rekomenduojame tai daryti efektyviausiu būdu.

„Local Run Manager“ saugos pataisos 1.0 versijos diegimo programos naudojimas

Paleista „Illumina MSI“ („Microsoft Installer“) programa atnaujins „Local Run Manager“ žiniatinklio serverio konfigūraciją, kad būtų išvengta bet kokio naudotojo įkelto turinio vykdymo ir būtų užblokuota visa nuotolinė prieiga prie „Local Run Manager“ žiniatinklio sąsajos iš LAN tinklo jungčių.

Naudotojams, kurie naudoja „Local Run Manager“ žiniatinklio sąsają, norėdami nuotoliniu būdu pasiekti instrumentus, ši darbo eiga nustos veikti įdiegus pataisą. „Illumina“ ketina vėliau atkurti šią funkciją, išleisdama nuolatinę programinės įrangos pataisą. Jei dėl to nutrūksta nustatyti darbo procesai, susisiekite adresu techsupport@illumina.com dėl tolesnės pagalbos.

MSI diegimo programa taikoma visoms „Local Run Manager“ versijoms ir automatiškai nustato tinkamą pataisą pagal instrumente / kompiuteryje įdiegtą „Local Run Manager“ versiją.

Ši MSI diegimo programa taip pat sukurs audito failą, rodantį, kad šis rizikos mažinimo būdas įgyvendintas, kartu su laiko žyma, nurodančia tinkamą diegimą.

MSI diegimo programos paleidimas: pirmą kartą paleidus MSI diegimo programą, ji pataisys sistemą ir sukurs audito failą su atlikimo laiku.

Dar kartą paleidus MSI diegimo programą, bus parodyta parinktis **Repair** (Taisyti); naudotojas turės galimybę iš naujo pritaikyti arba atšaukti pataisą. Pastaba: atšaukus pataisą, instrumento konfigūracija bus nesaugi.

„Local Run Manager“ saugos pataisos taikymas

Norėdami įdiegti pataisą, atlikite toliau nurodytus veiksmus.

1. Prisijunkite prie sistemos naudodami administratoriaus paskyrą (pvz., sbsadmin).

   „Illumina“ rekomenduoja pataisą taikyti, kai instrumentas neveikia. Jei instrumentas vykdo procedūrą, pataisą reikia pritaikyti iš karto po jos.

2. Raskite į sistemą atsisiųstą pataisą.
3. Perkelkite pataisos diegimo programą į `C:\Illumina` aplanką (netaikoma programinės įrangos apribojimų politika).
4. Dukart spustelėkite diegimo programos piktogramą, kad paleistumėte sąsają.
5. Kai programa įkeliama, spustelėkite **Next** (Toliau), kad pradėtumėte pataisos diegimą.
6. Diegimo užbaigimo ekrane spustelėkite **Finish** (Baigti).

Jei reikia patikrinti diegimo ataskaitą, žr. *Patikrinimas* 5 psl.

Diegimo pabaigoje būtina paleisti sistemą iš naujo.

Tvarkymas

Įvykus klaidai, klientas gali sutvarkyti įdiegimą vadovaudamasis toliau pateiktais nurodymais.

1. Prisijunkite prie sistemos naudodami administratoriaus paskyrą (pvz., sbsadmin).
2. Raskite į sistemą atsisiųstą pataisą.
3. Perkelkite pataisos diegimo programą į `C:\Illumina` aplanką (netaikoma programinės įrangos apribojimų politika).
4. Dukart spustelėkite diegimo programos piktogramą, kad paleistumėte sąsają.
5. Diegimo programa automatiškai nustatys, ar konfigūravimo įrankis buvo vykdytas anksčiau, ir pateiks naujas parinktis:
   a. „Change“ (Keisti): pažymėta pilka spalva ir nepasiekiama;
   b. „Repair“ (Tvarkyti): ištaisomos klaidos ir suteikiama galimybė pakeisti konfigūraciją;
   c. „Remove“ (Šalinti): pataisa pašalinama ir atkuriama numatytoji konfigūracija (žr. skiltį *Šalinimas* 5 psl.).
6. Diegimo užbaigimo ekrane spustelėkite **Finish** (Baigti).

Jei reikia patikrinti diegimo ataskaitą, žr. *Patikrinimas* 5 psl.

Diegimo pabaigoje būtina paleisti sistemą iš naujo.

Šalinimas

Pašalinus pataisą, panaikinami programos pagrindinio kompiuterio konfigūracijos failo pakeitimai.

1. Prisijunkite prie sistemos naudodami administratoriaus paskyrą (pvz., sbsadmin).
2. Raskite į sistemą atsisiųstą pataisą.
3. Perkelkite pataisos diegimo programą į `C:\Illumina` aplanką (netaikoma programinės įrangos apribojimų politika).
4. Dukart spustelėkite diegimo programos piktogramą, kad paleistumėte sąsają.
5. Pasirinkite **Remove** (Pašalinti) norėdami pašalinti pataisą ir grąžinti visus nustatymus į numatytuosius.
6. Pasirinkite **Remove** (Pašalinti) norėdami patvirtinti pataisos šalinimo parinktį ir grąžinti visus nustatymus į numatytuosius.

Tai atlikus, sistema taps nesaugi ir pažeidžiama išpuolio. Prieš pašalinant pataisą, labai rekomenduojama apsvarstyti visus techninius padarinius, dėl kurių norima pašalinti pataisą.

7. Diegimo užbaigimo ekrane spustelėkite **Finish** (Baigti).

Jei reikia patikrinti diegimo ataskaitą, žr. *Patikrinimas* 5 psl.

Diegimo pabaigoje rekomenduojama paleisti sistemą iš naujo.

Patikrinimas

Jei reikia patikrinti diegimą, bus sugeneruotas patikrinimo failas, kuriame yra datos ir laiko žyma, įdiegtos „Local Run Manager“ programos versija ir kitos pagrindinės patikros reikšmės. Norėdami gauti šį failą, susisiekite adresu techsupport@illumina.com.

Papildomos rizikos mažinimo ir saugumo rekomendacijos

Saugus RUO instrumentų ir Dx medicinos priemonių diegimas priklauso nuo saugumo lygių. „Illumina“ primygtinai rekomenduoja, kad instrumentai ir priemonės būtų naudojami mažiausiame potinklyje arba saugioje aplinkoje su patikimomis priemonėmis. Labai patartina naudoti užkardas ir kitas tinklo strategijas, kad būtų apribota prieiga prie kitų gaunamų ir siunčiamų duomenų.

Taip pat žiūrėkite toliau pateiktas rekomendacijas.

- Įjunkite „Transport Layer Security“ (TLS), kad užtikrintumėte, jog visi ryšiai už instrumento ribų būtų užšifruoti.
  - Norėdami įjungti „Transport Layer Security“ (TLS), žr. „Local Run Manager“ programinės įrangos vadovą.

Alternatyvos

Jei dėl kokių nors priežasčių pataisos paleisti neįmanoma, riziką galima sumažinti neautomatiškai toliau nurodytais būdais.

- Išjunkite nuotolinę prieigą prie „Local Run Manager“ pridėdami „Windows“ užkardos taisykles, blokuojančias gaunamus 80 ir 443 prievadų ryšius.
  „MSI Installer“ automatiškai blokuos nuotolinius gaunamus ryšius „Local Run Manager“ žiniatinklio serverio konfigūracijoje. Dar vienas tą patį užtikrinantis neautomatinis rizikos mažinimo būdas – įdiegti „Windows“ užkardos konfigūraciją, kad būtų blokuojami įeinantys `HTTP (TCP:80)` ir `HTTPS (TLS, TCP:443)` jungčių ryšiai.
  Įdiegus „Local Run Manager“ programą, ją galima pasiekti tik tame kompiuteryje, kuriame ji įdiegta; programa nebebus prieinama kituose kompiuteriuose, prijungtuose prie to paties tinklo.

Jei naudotojo darbo procesas apima nuotolinę prieigą prie „Local Run Manager“, ši funkcija neveiks.

- Sumažinkite kitų tinklo įrenginių skaičių.
  Sukonfigūravus tinklą taip, kad kitų tinklo įrenginių, galinčių užmegzti ryšį su paveiktu instrumentu, skaičius būtų kuo mažesnis, sumažės galimybė išnaudoti pažeidžiamumą. Kuo mažiau jungčių prie sistemos, tuo mažiau prieigos galimybių.
  Gali reikėti pasikonsultuoti su vietinėmis informacijos saugos ar IT tarnybomis.
- Atjunkite instrumentą nuo tinklo.
  Jei visa kita jau išbandėte, paskutinis rizikos mažinimo būdas – visiškai atjungti instrumentą nuo tinklo. Tokiu atveju nebeliks prieigos prie „Illumina Cloud“ / „SaaS“ paslaugų, tokių kaip „Proactive“ ir „BaseSpace® Sequence Hub“, taip pat įprastų genominių duomenų perkėlimo darbo procesų.
  Gali reikėti pasikonsultuoti su vietinėmis informacijos saugos ar IT tarnybomis.

Galbūt neteisėtos prieigos tyrimas

Toliau nurodyti veiksmai gali padėti instrumento operatoriui nustatyti, ar neteisėtas naudotojas prisijungė prie sistemos.

1. Patikrinkite, ar IIS žurnaluose, saugomuose `C:\inetpub\logs\LogFiles\W3SVC1`, nėra nejprastų skambučių.
   - Įprasti skambučiai į „Local Run Manager“ žiniatinklio serverį atrodo taip:

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

   - Nejprasti skambučiai į „Local Run Manager“ žiniatinklio serverį gali atrodyti, pavyzdžiui, taip:

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

2. Patikrinkite, ar IIS žurnale nėra ženklų, rodančių kito turinio, nei deklaracijos failai, POST įkėlimą. Pavyzdžiui, toliau nurodyti skambučiai rodytų įtartiną veiklą.

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

3. Jei įdiegta apsaugos nuo virusų / kenkėjiškų programų programa, patikrinkite, ar programinės įrangos žurnaluose nėra neįprastos veiklos ženklų.
4. Patikrinkite, ar „Windows“ žurnaluose nėra neįprastų klaidų pranešimų ženklų.
   Jei grėsmės sukėlėjui pavyktų prisijungti administratoriaus teisėmis, jis gali pakeisti arba panaikinti visus vietinius instrumento žurnalus ir įvykius.

Patikrinkite, ar nėra galinių taškų, kuriuos sistema galėjo bandyti pasiekti. Tikėtinų išeinančių ryšių sąrašą rasite dalyje Valdymo kompiuterio užkarda.

Dėl reikalingos techninės pagalbos kreipkitės į „Illumina“ techninės priežiūros skyrių.

Keitimo istorija

Dokumentas	Data	Keitimo aprašas
Dokumento Nr. 200017330 02 v.	2022 m. balandžio mėn.	Pridėta rekomendacija taikyti pataisą, kai instrumentas neveikia. Pridėta instrukcija įdiegus pataisą iš naujo paleisti instrumentą. Pataisytas 01 versijos keitimo istorijos aprašas.
Dokumento Nr. 200017330 01 v.	2022 m. balandžio mėn.	Pakeistas dokumento pavadinimas į „LRM programinės įrangos 1.0 pataisos instrukcijų vadovas“. Pašalinti visi v1.0.1 paminėjimai. Pridėtas skyrius apie galbūt neteisėtos prieigos tyrimą.
Dokumento Nr. 200017330 00 v.	2022 m. kovo mėn.	Pirmasis leidimas.