LRM Software Patch 1.0

illumina®

Talimat Kılavuzu

Giriş

Illumina® bir süre önce Local Run Manager yazılımında bir güvenlik açığı bulunduğunu fark etti ve bu güvenlik açığının uzaktan suistimal edilmesine karşı koruma sağlamak için bir yazılım yaması sundu.

Local Run Manager bağımsız bir yazılım uygulamasıdır ve aşağıdaki sistemlerde varsayılan yapılandırmanın bir parçası olarak sunulmaktadır:

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

*İn vitro tanı amaçlı kullanım içindir.

Bu kılavuz, yukarıda listelenen Illumina cihazları için ve Local Run Manager'ın bağımsız versiyonunun yüklü olduğu cihaz dışı bilgisayarlar için geçerlidir.

Güvenlik açığı, riski azaltılmamış CVSS puanı 10,0 Kritik olan Kimliği Doğrulanmamış Uzak Komut Yürütme (RCE) `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H` sorunudur.

Yetkisiz bir kullanıcının bir veya daha fazla cihaza erişmesi ve uzak erişim saldırısı gerçekleştirmesi olasılığına karşı güvenliği sağlamak için yukarıda listelenen cihazlarda aşağıda belirtilen risk azaltma adımlarının uygulanması gerekir.

Herhangi bir nedenle yükleyicinin çalıştırılamaması durumunda bu belgenin sonunda yer alan ilave risk azaltma yöntemleri bölümüne başvurun veya ek yardım için techsupport@illumina.com adresi ile iletişime geçin.

Yamayı indirme veya bir kopyasını talep etme seçenekleri için Local Run Manager Güncellemesini Alma bölümüne bakın.

- **v1.0.0 yama** - Local Run Manager web yapılandırmasını günceller ve uzak Internet Information Services (IIS) erişimini devre dışı bırakır.

Local Run Manager Güvenlik Yamasını Edinme

Local Run Manager Güvenlik Yamasını edinmek için dört (4) seçenek sunulmaktadır.

Seçenek 1—Doğrudan cihazınıza indirin

Local Run Manager Güvenlik Güncellemesini almanın en hızlı yolu, doğrudan barındırma web sitesinden cihaza indirmektir.

1. Yama yükleyicisini, güvenli e-posta ile sağlanan bağlantıdan cihazınıza indirin.
2. Dosyayı cihazdaki `C:\Illumina` klasörüne aktarın.
3. *Local Run Manager Güvenlik Yamasını Uygulama*, sayfa 3 bölümünde belirtilen talimatları uygulayın.

Seçenek 2—Yama yükleyicisini bilgisayara indirin ve USB sürücü/paylaşılan klasör aracılığıyla cihaza aktarın

Güvenlik yamasını cihaza indiremezseniz ayrı bir bilgisayara indirip daha sonra cihaza aktarmanızı öneririz.

Kullanmadan önce Güvenlik temsilcilerinizle birlikte USB sürücünün sağlamlığını doğrulayın. (Önerilir)

1. Yama yükleyicisini, güvenli e-posta ile sağlanan bağlantıdan bilgisayarınıza veya dizüstü bilgisayarınıza indirin.
2. İndirilen yama yükleyicisini USB sürücüye veya bilgisayardaki paylaşılan klasöre kopyalayın.
3. USB sürücü için, sürücüyü Cihaza takın.
4. Yama yükleyicisini USB sürücüden veya paylaşılan klasörden cihazdaki `C:\Illumina` klasörüne kopyalayın.
5. *Local Run Manager Güvenlik Yamasını Uygulama*, sayfa 3 bölümünde belirtilen talimatları uygulayın.

Seçenek 3—Teknik Destek Talep Edin

Bir Illumina Teknik Destek temsilcisi, aşağıdaki yöntemlerden birini kullanarak yama uygulama sürecinde size kılavuzluk sağlayacaktır:

- Teknik Destek Uzak oturumu

  Bir Teknik Destek temsilcisi, analiz cihazına uzaktan bağlanacak ve müşteri adına yamayı yükleyecektir.

  Sistem uzak erişime açık olmalıdır. Herhangi bir sorunuz varsa yerel BT temsilcinizden yardım isteyin.

- Kılavuzlu Talimatlar

  Bir Teknik Destek temsilcisi, telefonla kılavuzlu talimatlar verecektir. Yardım için lütfen yerel Teknik Destek temsilcinizle iletişime geçin.

Seçenek 4—Illumina'dan önceden yapılandırılmış sürücü sipariş edin

Müşteriler hiçbir ücret ödemeksizin yazma korumalı USB sürücü sipariş edebilir. Yama yüklü sürücü sipariş etmek için lütfen techsupport@illumina.com adresi ile iletişime geçin.

Teslimatın zamanında yapılmasını etkileyebilecek sevkiyat ya da envanter gecikmeleri söz konusu olabilir. Sistemleri daha kısa süre içinde koruma altına almak için, sistemlerin en etkili çözüm yolunu sunacak yöntemle korumaya alınması önemle tavsiye edilir.

Local Run Manager Security Patch v.1.0 Yükleyiciyi Çalıştırma

Illumina MSI (Microsoft Yükleyicisi) yürütüldüğünde, kullanıcı tarafından yüklenen tüm içeriklerin yürütülmesini engellemek ve LAN ağ bağlantılarından Local Run Manager web arayüzüne tüm uzak erişimleri engellemek üzere Local Run Manager web sunucusu yapılandırmasını günceller.

Bu yamanın yüklenmesinin ardından, cihazlara uzak erişim için Local Run Manager web arayüzünü kullanan kullanıcılar için bu iş akışı işlevsiz hale gelecektir. Illumina bu soruna ilişkin kalıcı bir yazılım düzeltmesi ile bu işlevi daha sonra geri yüklemeyi planlamaktadır. Bu durum, belirlenmiş iş akışlarında aksaklığa neden olursa lütfen daha fazla yardım için techsupport@illumina.com adresi ile iletişime geçin.

MSI yükleyicisi, Local Run Manager'ın tüm versiyonları için kullanılabilir ve cihazınızda/bilgisayarınızda yüklü olan Local Run Manager versiyonuna göre doğru düzeltmeyi otomatik olarak belirler.

Bu MSI yükleyici, uygun yükleme işleminin gerçekleştiğini yansıtan bir zaman damgası ile birlikte bu risk azaltma yönteminin uygulandığını gösteren bir denetim dosyası oluşturur.

MSI Yükleyicisi – MSI Yükleyicisi ilk çalıştırıldığında, yükleyici sisteme yama yükler ve tamamlanma saati ile birlikte bir denetim dosyası oluşturur.

MSI Yükleyicisi yeniden çalıştırıldığında bir **Repair** (Onarım) seçeneği ile kullanıcıya yamayı yeniden uygulama veya geri alma seçeneği sunulur. Not: Yamanın geri alınması, cihaz yapılandırmasının güvenli olmamasına neden olur.

Local Run Manager Güvenlik Yamasını Uygulama

Yamayı yüklemek için:

1. Bir yönetici hesabıyla (ör. sbsadmin) sistemde oturum açın.

   Illumina, yamanın cihaz çalışmıyorken uygulanmasını önerir. Cihaz bir çalıştırma yürütüyorsa yama, çalıştırma tamamlandıktan hemen sonra uygulanmalıdır.

2. Sisteme indirilen yamayı bulun.

3. Yama yükleyicisini `C:\Illumina` klasörüne taşıyın (Yazılım Kısıtlama Politikasından muaf tutulur).
4. Arayüzü başlatmak için yükleyici simgesine çift tıklayın.
5. Uygulama yüklendiğinde, yama yükleme işlemini başlatmak için **Next** (Sonraki) seçeneğini belirleyin.
6. Installation Completion (Yükleme Tamamlandı) ekranında **Finish** (Bitir) seçeneğini belirleyin.

Yükleme doğrulama raporu gerekiyorsa lütfen *Doğrulama*, sayfa 5 bölümüne bakın.

Yükleme işleminin sonunda yeniden başlatma yapılması gerekir.

Onarım

Hata oluşması durumunda müşteri, aşağıdaki talimatları uygulayarak yükleme onarımını yürütebilir:

1. Bir yönetici hesabıyla (ör. sbsadmin) sistemde oturum açın.
2. Sisteme indirilen yamayı bulun.
3. Yama yükleyicisini `C:\Illumina` klasörüne taşıyın (Yazılım Kısıtlama Politikasından muaf tutulur).
4. Arayüzü başlatmak için yükleyici simgesine çift tıklayın.
5. Yükleyici, yapılandırma aracının daha önce yürütülüp yürütülmediğini otomatik olarak algılar ve yeni seçenekler sunar:
   a. Change (Değiştir): Soluk renklidir ve kullanılamaz
   b. Repair (Onarım): Hataları onarır ve yeniden yapılandırma için seçenekler sunar.
   c. Remove (Kaldır): Yamayı kaldırır ve varsayılan yapılandırmayı geri yükler (bkz. *Kaldırma*, sayfa 4)
6. Installation Completion (Yükleme Tamamlandı) ekranında **Finish** (Bitir) seçeneğini belirleyin.

Yükleme doğrulama raporu gerekiyorsa lütfen *Doğrulama*, sayfa 5 bölümüne bakın.

Yükleme işleminin sonunda yeniden başlatma yapılması gerekir.

Kaldırma

Yamanın kaldırılması, uygulama ana bilgisayar yapılandırma dosyasında yapılan değişikliklerin geri alınmasını sağlar.

1. Bir yönetici hesabıyla (ör. sbsadmin) sistemde oturum açın.
2. Sisteme indirilen yamayı bulun.
3. Yama yükleyicisini `C:\Illumina` klasörüne taşıyın (Yazılım Kısıtlama Politikasından muaf tutulur).
4. Arayüzü başlatmak için yükleyici simgesine çift tıklayın.
5. **Remove** (Kaldır) seçeneğini belirleyerek yamayı kaldırın ve tüm değerleri varsayılan ayarlara geri döndürün.
6. **Remove** (Kaldır) seçeneğini belirleyerek yamayı kaldırma ve tüm değerleri varsayılan ayarlara geri döndürme seçeneğini doğrulayın.

Bu ayar, sistemin güvensiz ve saldırı riski altında olmasına neden olur. Kaldırma seçeneğini kullanmadan önce yamanın kaldırılmasına yol açan tüm teknik sorunların çözülmesi önemle tavsiye edilir.

7. Installation Completion (Yükleme Tamamlandı) ekranında **Finish** (Bitir) seçeneğini belirleyin.

Yükleme doğrulama raporu gerekiyorsa lütfen *Doğrulama*, sayfa 5 bölümüne bakın.

Yükleme işleminin sonunda yeniden başlatma yapılması önerilir.

Doğrulama

Yükleme işleminin doğrulanması gerekiyorsa bir tarih ve saat damgası, yüklenen Local Run Manager versiyonu ve diğer anahtar doğrulama değerlerini içeren bir doğrulama dosyası oluşturulur. Bu dosyayı almak için lütfen techsupport@illumina.com adresi ile iletişime geçin.

İlave Risk Azaltma ve Güvenlik Önerileri

RUO cihazların ve Dx tıbbi cihazların güvenli şekilde kullanıma alınması, güvenlik katmanlarına bağlıdır. Illumina, cihazların güvenilir cihazlarla birlikte en küçük ağ alt ağında ya da güvenlik bağlamında kullanıma alınmasını kesinlikle tavsiye etmektedir. Diğer gelen ve giden bağlantı erişimlerini kısıtlamak için güvenlik duvarlarının ve diğer ağ politikalarının kullanılması önemle tavsiye edilir.

İlave önerilerimiz:

- Tüm cihaz dışı iletişimlerin şifrelenmesini sağlamak için Taşıma Katmanı Güvenliği (TLS) özelliğini etkinleştirin.
  - Taşıma Katmanı Güvenliği (TLS) özelliğini etkinleştirmek için lütfen Local Run Manager Yazılım Kılavuzuna bakın.

Alternatif Seçenekler

Herhangi bir nedenle yama yürütülemiyorsa aşağıdaki manuel risk azaltma yöntemleri riski azaltacaktır:

- Gelen Port 80 ve 443 bağlantılarını engellemek için Windows güvenlik duvarı kurallarına ekleyerek Local Run Manager'a uzak erişimi devre dışı bırakın.
  MSI Yükleyicisi, Local Run Manager web sunucusu yapılandırmasında uzak gelen bağlantıları otomatik olarak engelleyecektir. Aynı sonucu elde edebileceğiniz bir manuel risk azaltma yöntemi olarak `HTTP (TCP:80)` ve `HTTPS (TLS, TCP:443)` bağlantılarına gelen bağlantıları engellemek için bir Windows güvenlik duvarı yapılandırması uygulayabilirsiniz.
  Uygulandıktan sonra Local Run Manager'a yalnızca Local Run Manager'ın yüklü olduğu bilgisayardan erişilebilir; aynı ağa bağlı diğer bilgisayarlardan erişilemez.

Kullanıcı iş akışında, Local Run Manager'a uzak bağlantı yapılması gerekiyorsa bu işlev çalışmaz.

- Diğer ağ cihazlarının sayısını en aza indirin.
  Etkilenen cihazla iletişim kurabilecek olan diğer ağ cihazlarının sayısını en aza indirmek üzere ağı yapılandırmanız, suistimal potansiyelinin azaltılmasını sağlar. Sisteme bağlantıların sayısı ne kadar az olursa erişim fırsatı o kadar az olur.

Bunu gerçekleştirmek için yerel Bilgi Güvenliği veya BT kaynaklarınıza danışmanız gerekebilir.

- Cihazı ağdan kaldırın.
  Başka hiçbir seçenek uygulanamazsa son risk azaltma yöntemi, cihazı tamamen ağdan kaldırmaktır. Bu işlem, Proactive ve BaseSpace® Sequence Hub gibi Illumina Cloud/SaaS hizmetlerine ve tipik genomik veri boşaltma iş akışlarına erişimi devre dışı bırakacaktır.
  Bunu gerçekleştirmek için yerel Bilgi Güvenliği veya BT kaynaklarınıza danışmanız gerekebilir.

Olası Yetkisiz Erişimin Araştırılması

Aşağıdaki adımlar, cihaz operatörünün yetkisiz bir kullanıcının sisteme erişip erişmediğini belirlemesine yardımcı olabilir:

1. Anormal çağrılar için `C:\inetpub\logs\LogFiles\W3SVC1` konumunda depolanan IIS günlüklerini inceleyin.
   - Local Run Manager web sunucusuna yapılan normal çağrılar şu şekilde görünür:
     ```
     GET http /normalresource.extension?normal-URI-decoration
     ```
   - Local Run Manager web sunucusuna yapılan anormal çağrılar örneğin şu şekilde görünebilir:
     ```
     POST http /hackertool.asp
     ```
2. IIS günlüğünü belirtim dosyaları dışında POST içerik yüklemesi işareti olup olmadığı açısından inceleyin. Örneğin, aşağıdaki çağrılar şüpheli aktivite belirtisidir:
   ```
   wscript
   shell
   wscript.network
   scripting.filesystemObject
   ```
3. Bir anti-virüs/kötü amaçlı yazılımdan koruma uygulaması yüklenmişse yazılım günlüklerini anormal davranış işaretleri olup olmadığı açısından kontrol edin.
4. Windows günlüklerini anormal hata mesajı işaretleri olup olmadığı açısından inceleyin.
   Bir tehdit aktörü yönetici haklarıyla birlikte erişim elde ederse tüm yerel cihaz günlüklerini ve olaylarını değiştirebilir ya da silebilir.

Sistemin erişmeyi denemiş olabileceği tüm uç noktaları kontrol edin. Beklenen giden bağlantıların listesi için Denetim Bilgisayarı Güvenlik Duvarına bakın.

Gerektiği şekilde yardım için Illumina Teknik Destek bölümü ile iletişim kurun.

Revizyon Geçmişi

Belge	Tarih	Değişiklik Açıklaması
Belge No 200017330 v02	Nisan 2022	Yamayı cihaz çalışmıyorken uygulama önerisi eklendi. Yama yüklemesinden sonra cihazın yeniden başlatılmasına yönelik talimat eklendi. v01 için revizyon geçmişi açıklaması düzeltildi.
Belge No 200017330 v01	Nisan 2022	Belge başlığı "LRM Software Patch 1.0 Talimat Kılavuzu" olarak değiştirildi. Tüm v1.0.1 ibareleri kaldırıldı. Olası yetkisiz erişimin araştırılmasına ilişkin bölüm eklendi.
Belge No 200017330 v00	Mart 2022	İlk sürüm.