

Guia de instruções

Introdução

A Illumina® tomou conhecimento de uma vulnerabilidade de segurança presente no software Local Run Manager e forneceu um patch de software para proteção contra a exploração remota dessa vulnerabilidade.

O Local Run Manager é um aplicativo de software autônomo e faz parte da configuração padrão nos seguintes sistemas:

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

*Para uso em diagnóstico in vitro.

Este guia se aplica aos instrumentos Illumina indicados acima e também aos computadores à exceção do instrumento em que a versão autônoma do Local Run Manager foi instalada.

A vulnerabilidade é uma execução de comando remoto (RCE, Remote Command Execution) não autenticado, com uma pontuação CVSS não mitigada de 10.0 Crítico, CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H.

As etapas de mitigação a seguir são exigidas nos instrumentos listados acima para proteção contra a possibilidade de um usuário não autorizado obter acesso a um ou mais instrumentos e executar um ataque de acesso remoto.

Se, por algum motivo, não for possível executar o instalador, consulte a seção de mitigações adicionais no final deste documento ou entre em contato com techsupport@illumina.com para obter ajuda adicional.

Consulte [Obter a atualização do Local Run Manager](#) para ver as opções de como baixar ou solicitar uma cópia do patch.

- **Patch v1.0.0** – atualizará a configuração da Web do Local Run Manager e desabilitará o acesso remoto aos serviços de informações da internet (IIS, Internet Information Services).

Obtenha o patch de segurança do Local Run Manager

Existem quatro (4) opções para a obtenção do patch de segurança do Local Run Manager.

Opção 1: baixe diretamente no seu instrumento

A maneira mais rápida de obter a atualização de segurança do Local Run Manager é baixá-la diretamente do site de hospedagem do instrumento.

1. Baixe o instalador do patch no link fornecido via e-mail seguro para seu instrumento.
2. Transfira o arquivo para a pasta `C:\Illumina` no instrumento.
3. Siga as instruções em [Aplicar o patch de segurança do Local Run Manager na página 4](#).

Opção 2: baixe o instalador do patch no computador e transfira-o para o instrumento por meio de uma unidade USB/pasta compartilhada

i | Se você não conseguir baixar o patch de segurança no instrumento, recomendamos baixá-lo em um computador separado e transferi-lo para o instrumento.

Verifique a integridade da unidade USB com os representantes de segurança antes de usá-la. (Recomendado)

1. Baixe o instalador do patch no link fornecido via e-mail seguro para o seu computador ou laptop.
2. Copie o instalador do patch baixado para a unidade USB ou a pasta compartilhada do computador.
3. No caso de unidade USB, conecte a unidade ao instrumento.
4. Copie o instalador do patch da unidade USB ou da pasta compartilhada para a pasta `C:\Illumina` no instrumento.
5. Siga as instruções em [Aplicar o patch de segurança do Local Run Manager na página 4](#).

Opção 3: acione o suporte técnico

Um representante do suporte técnico da Illumina orientará você ao longo do processo de aplicação de patch usando um dos seguintes métodos:

- Login remoto do suporte técnico

Um representante do suporte técnico poderá acessar o analisador remotamente e instalar o patch em nome do cliente.

i | O sistema deve ser acessível remotamente. Se você tiver alguma dúvida, peça ajuda ao representante de TI local.

- Instruções guiadas

Um representante do suporte técnico fornecerá instruções guiadas pelo telefone. Entre em contato com o representante do suporte técnico local para obter ajuda.

Opção 4: solicite uma unidade pré-configurada da Illumina

Uma unidade USB protegida contra gravação pode ser solicitada pelo cliente sem custo. Para solicitar a unidade com o patch instalado, entre em contato com techsupport@illumina.com.

i | É possível que haja atrasos nas remessas ou no estoque que possam afetar o cronograma da entrega. Para uma proteção mais imediata dos sistemas, é altamente recomendável que eles sejam protegidos pelo método que oferecerá o caminho de resolução mais eficiente.

Aplique o instalador do patch de segurança do Local Run Manager v.1.0

O instalador MSI (instalador da Microsoft) da Illumina, quando executado, corrigirá a configuração do servidor Web do Local Run Manager para impedir a execução de qualquer conteúdo carregado pelo usuário e bloquear todo o acesso remoto à interface da Web do Local Run Manager por meio de conexões de rede LAN.

i | Para os usuários que usam a interface da Web do Local Run Manager para acessar instrumentos remotamente, esse fluxo de trabalho deixará de funcionar após a instalação desse patch. A Illumina pretende restaurar essa funcionalidade futuramente com uma correção permanente de software para esse problema. Se isso causar uma interrupção nos fluxos de trabalho estabelecidos, entre em contato com techsupport@illumina.com para obter ajuda adicional.

O instalador MSI é aplicável a todas as versões do Local Run Manager e determinará automaticamente a correção mais adequada com base na versão do Local Run Manager instalada no instrumento/computador. Esse instalador MSI também criará um arquivo de auditoria mostrando que essa mitigação foi implementada, bem como um carimbo de data/hora para refletir a instalação adequada.

Execução do instalador MSI – na primeira vez que o instalador MSI for executado, ele corrigirá o sistema e criará um arquivo de auditoria com a hora da conclusão.

i | Uma nova execução do instalador MSI apresentará uma opção **Repair** (Reparar): o usuário terá a opção de reaplicar ou reverter o patch. Observação: a reversão do patch resultará em uma configuração não segura do instrumento.

Aplicar o patch de segurança do Local Run Manager

Para instalar o patch:

1. Faça login no sistema usando uma conta de administrador (por exemplo, sbsadmin).

i | A Illumina recomenda que o patch seja aplicado quando o instrumento não estiver em execução. Se o instrumento estiver processando uma execução, o patch deverá ser aplicado imediatamente após a conclusão da execução.

2. Localize o patch que foi baixado no sistema.
3. Transfira o instalador do patch para a pasta `C:\Illumina` (isenta da Política de restrição de software).
4. Clique duas vezes no ícone do instalador para iniciar a interface.
5. Quando o aplicativo for carregado, selecione **Next** (Avançar) para iniciar a instalação do patch.
6. Na tela Installation Completion (Conclusão da instalação), selecione **Finish** (Concluir).

i | Caso uma verificação do relatório de instalação seja exigida, consulte [Verificação na página 5](#).

i | É necessária uma reinicialização ao final da instalação.

Reparo

Em caso de erro, o cliente pode executar o reparo da instalação seguindo as instruções abaixo:

1. Faça login no sistema usando uma conta de administrador (por exemplo, sbsadmin).
2. Localize o patch que foi baixado no sistema.
3. Transfira o instalador do patch para a pasta `C:\Illumina` (isenta da Política de restrição de software).
4. Clique duas vezes no ícone do instalador para iniciar a interface.
5. O instalador detectará automaticamente se a ferramenta de configuração foi executada anteriormente e apresentará novas opções:
 - a. Change (Alterar): em cinza e indisponível.
 - b. Repair (Reparar): repara os erros e oferece opções para reconfiguração.
 - c. Remove (Remover): desinstala o patch e o restaura para a configuração padrão (consulte [Desinstalação na página 5](#)).
6. Na tela Installation Completion (Conclusão da instalação), selecione **Finish** (Concluir).


i | Caso uma verificação do relatório de instalação seja exigida, consulte [Verificação na página 5](#).

i | É necessária uma reinicialização ao final da instalação.


Desinstalação

A desinstalação do patch reverterá as modificações feitas no arquivo de configuração do host do aplicativo.

1. Faça login no sistema usando uma conta de administrador (por exemplo, sbsadmin).
2. Localize o patch que foi baixado no sistema.
3. Transfira o instalador do patch para a pasta C:\Illumina (isenta da Política de restrição de software).
4. Clique duas vezes no ícone do instalador para iniciar a interface.
5. Selecione **Remove** (Remover) para desinstalar o patch e reverter todos os valores para as configurações padrão.
6. Selecione **Remove** (Remover) para verificar a opção de desinstalar o patch e reverter todos os valores para as configurações padrão.

 Essa configuração deixará o sistema não seguro e em risco de ataque. É altamente recomendável que qualquer impacto técnico que cause a opção de remover o patch seja resolvido antes de optar por desinstalar.

7. Na tela Installation Completion (Conclusão da instalação), selecione **Finish** (Concluir).

 Caso uma verificação do relatório de instalação seja exigida, consulte [Verificação na página 5](#).

 É recomendável uma reinicialização ao final da instalação.

Verificação

Se houver necessidade de verificar a instalação, será gerado um arquivo de verificação que inclui um carimbo de data/hora, a versão do Local Run Manager instalado e outros valores fundamentais da verificação. Para obter esse arquivo, entre em contato com techsupport@illumina.com.

Recomendações adicionais de mitigação e segurança

A implantação segura de instrumentos somente para uso em pesquisa (RUO, Research Use Only) e dispositivos médicos Dx depende de camadas de segurança. A Illumina recomenda, veementemente, que instrumentos e dispositivos sejam implantados na menor sub-rede de rede ou contexto de segurança com outros dispositivos confiáveis. O uso de firewalls e outras políticas de rede para restringir outros acessos de entrada e saída é altamente recomendável.

Também recomendamos:

- Habilite o protocolo TLS (Transport Layer Security, Segurança da camada de transporte) para garantir que todas as comunicações à exceção do instrumento sejam criptografadas.
 - Para habilitar o TLS, consulte o Guia do software Local Run Manager.

Opções alternativas

Se, por algum motivo, a execução do patch não for uma opção, os seguintes métodos de mitigação manual reduzirão o risco:

- Desative o acesso remoto ao Local Run Manager adicionando regras de firewall do Windows para bloquear as conexões de entrada das portas 80 e 443.
O Instalador MSI bloqueará automaticamente as conexões de entrada remotas na configuração do servidor Web do Local Run Manager. Uma mitigação manual que obtém o mesmo resultado é a implementação de uma configuração de firewall do Windows para bloquear as conexões de entrada para HTTP (TCP:80) e HTTPS (TLS, TCP:443).
Após a implementação, o Local Run Manager poderá ser acessado apenas no computador em que está instalado; ele não poderá mais ser acessado de outros computadores conectados à mesma rede.

i | Se o fluxo de trabalho do usuário envolver o acesso remoto ao Local Run Manager, essa funcionalidade não estará mais disponível.

- Minimize o número de outros dispositivos de rede.
Configurar a rede para minimizar o número de outros dispositivos de rede que podem se comunicar com o instrumento afetado reduzirá a possibilidade da exploração. Quanto menos conexões disponíveis para o sistema, menos oportunidades disponíveis para acesso.
Essa execução pode exigir uma consulta aos recursos locais de Segurança da Informação ou de TI.
- Remova o instrumento da rede.
Se nenhuma outra opção for viável, a mitigação final será a remoção completa do instrumento da rede. Isso desabilitará o acesso aos serviços Illumina Cloud/SaaS, como o Proactive e BaseSpace® Sequence Hub, e fluxos de trabalho típicos de descarga de dados de genômica.
Essa execução pode exigir uma consulta aos recursos locais de Segurança da Informação ou de TI.

Investigação de possível acesso não autorizado.

As etapas a seguir podem ajudar o operador do instrumento a determinar se um usuário não autorizado acessou o sistema:

1. Examine os registros dos IIS armazenados em `C:\inetpub\logs\LogFiles\W3SVC1` quanto a chamadas anormais.
 - Chamadas normais para o servidor Web do Local Run Manager aparecem como a seguir:

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

- Chamadas anormais para o servidor Web do Local Run Manager aparecem, por exemplo, como:

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

2. Examine o registro dos IIS quanto a sinais de uploads de POST de conteúdo diferente do conteúdo dos arquivos de manifesto. Por exemplo, as seguintes chamadas indicariam atividade suspeita:

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

3. Se um aplicativo antivírus/antimalware estiver instalado, verifique os registros do software quanto a sinais de comportamento anormal.
4. Examine os registros do Windows quanto a sinais de mensagens de erro anormais.
Se um agente de ameaças obtivesse acesso com direitos de administrador, ele teria a capacidade de alterar ou excluir todos os registros e eventos do instrumento local.

Verifique todos os pontos de extremidade que o sistema possa ter tentado acessar. Para obter uma lista das conexões de entrada esperadas, consulte [Firewall do computador de controle](#).

Entre em contato com o suporte técnico da Illumina para obter ajuda, conforme necessário.

Histórico de revisões

Documento	Data	Descrição da alteração
Documento n.º 200017330 v02	Abril de 2022	Adicionada recomendação para aplicar o patch quando o instrumento não estiver em execução. Adicionada instrução de que é necessário reiniciar o instrumento após a instalação do patch. Corrigida a descrição do histórico de revisões para a v01.
Documento n.º 200017330 v01	Abril de 2022	Alterado o título do documento para Guia de instruções do patch de software do LRM 1.0 Removida qualquer menção à v1.0.1. Adicionada uma seção para abordar a investigação de possível acesso não autorizado.
Documento n.º 200017330 v00	Março de 2022	Versão inicial.

Este documento e seu conteúdo são de propriedade da Illumina, Inc. e de suas afiliadas ("Illumina") e destinam-se exclusivamente ao uso contratual de seu cliente com relação ao uso dos produtos descritos neste documento e para nenhuma outra finalidade. Este documento e seu conteúdo não devem ser usados ou distribuídos para nenhuma outra finalidade nem comunicados, divulgados ou reproduzidos de nenhuma forma sem o consentimento prévio por escrito da Illumina. A Illumina não concede nenhuma licença sob seus direitos de patente, marca registrada, direitos autorais ou lei comum nem direitos semelhantes de terceiros por meio deste documento.

As instruções neste documento devem ser estrita e explicitamente seguidas por pessoal devidamente treinado e qualificado para garantir o uso adequado e seguro dos produtos descritos neste documento. Todo o conteúdo deste documento deve ser lido e compreendido por completo antes da utilização de tais produtos.

NÃO LER COMPLETAMENTE E NÃO SEGUIR EXPLICITAMENTE TODAS AS INSTRUÇÕES AQUI CONTIDAS PODE RESULTAR EM DANOS AO(S) PRODUTO(S), FERIMENTOS A PESSOAS, INCLUSIVE USUÁRIOS OU OUTROS, E DANOS A OUTROS BENS, ANULANDO TODA GARANTIA APLICÁVEL AO(S) PRODUTO(S).

A ILLUMINA NÃO SE RESPONSABILIZA POR QUALQUER PROBLEMA CAUSADO PELO USO INDEVIDO DO(S) PRODUTO(S) MENCIONADO(S) ACIMA (INCLUINDO PARTES SEPARADAS OU O SOFTWARE).

© 2022 Illumina, Inc. Todos os direitos reservados.

Todas as marcas comerciais pertencem à Illumina, Inc. ou aos respectivos proprietários. Para obter informações específicas sobre marcas comerciais, consulte www.illumina.com/company/legal.html.