Patch de software do LRM 1.0

illumina®

Guia de instruções

Introdução

A Illumina® tomou conhecimento de uma vulnerabilidade de segurança presente no software Local Run Manager e providenciou um patch de software para oferecer proteção contra aproveitamentos remotos indevidos desta vulnerabilidade.

O Local Run Manager é uma aplicação de software independente e faz parte da configuração predefinida dos seguintes sistemas:

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

*Para utilização em diagnóstico in vitro.

Este guia aplica-se aos instrumentos Illumina indicados acima e também a computadores fora do instrumento com a versão autónoma do Local Run Manager instalada.

A vulnerabilidade é uma execução remota de código (Remote Command Execution, RCE) não autenticada com um índice CVSS não mitigado de 10.0 Crítico, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H`.

Os passos de mitigação que se seguem são obrigatórios nos instrumentos indicados acima de modo a proteger os mesmos da possibilidade de um utilizador não autorizado aceder a um ou mais instrumentos e executar um ataque de acesso remoto.

Se por algum motivo não for possível executar o ficheiro de instalação, consulte a secção de mitigações adicionais no fim deste documento ou contacte techsupport@illumina.com para obter mais assistência.

Consulte as opções para transferir ou pedir uma cópia do patch em Obter a atualização do Local Run Manager .

- **Patch v1.0.0** — Atualiza a configuração Web do Local Run Manager e desativa o acesso remoto dos Serviços de Informação Internet (Internet Information Services, IIS).

Obter o patch de segurança do Local Run Manager

Estão disponíveis quatro (4) opções para obter o patch de segurança do Local Run Manager.

Opção 1 — Transferir o mesmo diretamente para o seu instrumento

A forma mais rápida de obter a atualização de segurança do Local Run Manager é transferi-la diretamente a partir do website de alojamento do instrumento.

1. Transfira o ficheiro de instalação do patch a partir da ligação fornecida através de e-mail seguro para o seu instrumento.
2. Transfira o ficheiro 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 — Transferir o ficheiro de instalação do patch para o computador e depois para o instrumento através da pen USB/pasta partilhada

Caso não transfira o patch de segurança para o instrumento, recomendamos que o transfira para o computador separado e, depois, para o instrumento.

Verifique a integridade da pen USB com os seus representantes de Segurança antes de a utilizar. (recomendado)

1. Transfira o ficheiro de instalação do patch a partir da ligação fornecida através de e-mail seguro para o seu computador.
2. Copie o ficheiro de instalação do patch transferido para a pen USB ou a pasta partilhada do computador.
3. Se utilizar uma pen USB, ligue-a ao Instrumento.
4. Copie o ficheiro de instalação do patch da pen USB ou da pasta partilhada 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 — Solicitar suporte técnico

Um representante do Suporte Técnico da Illumina irá orientá-lo na aplicação do patch utilizando um dos seguintes métodos:

- Início de sessão remoto com Suporte Técnico

  Um representante do Suporte Técnico irá aceder remotamente ao analisador e instalar o patch em nome do cliente.

  O sistema tem de permitir o acesso remoto. Se tiver dúvidas, peça assistência ao seu representante de TI local.

- Instruções orientadas
  Um representante do Suporte Técnico irá fornecer instruções orientadas pelo telefone. Contacte o seu representante de Suporte Técnico para obter assistência.

Opção 4 — Encomendar uma pen pré-configurada da Illumina

O cliente pode encomendar gratuitamente uma pen USB protegida contra escrita. Para encomendar a pen com o patch instalado, contacte techsupport@illumina.com.

Pode haver atrasos com os envios ou o inventário que afetem o prazo de entrega. Para proteger os sistemas de forma mais imediata, recomendamos vivamente que os sistemas sejam protegidos pelo método que oferece o caminho de resolução mais eficaz.

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

O Illumina MSI (Microsoft Installer), quando executado, irá atualizar a configuração do servidor Web do Local Run Manager para evitar a execução de qualquer conteúdo enviado por utilizadores e bloquear todos os acessos remotos à interface Web do Local Run Manager a partir de ligações de rede LAN.

Para quem utiliza a interface Web do Local Run Manager para aceder remotamente a instrumentos, este fluxo de trabalho irá deixar de funcionar após a instalação deste patch. A Illumina tenciona restaurar esta funcionalidade mais tarde com a correção permanente de software para este problema. Se esta ação provocar uma interrupção dos fluxos de trabalho estabelecidos, contacte techsupport@illumina.com para obter mais assistência.

O MSI Installer é aplicável a todas as versões do Local Run Manager e irá determinar automaticamente a correção adequada com base na versão do Local Run Manager instalada no instrumento/computador.

Este MSI Installer irá também criar um ficheiro de auditoria que indica que esta mitigação foi implementada juntamente com um carimbo de data/hora para refletir a instalação correta.

Executar o MSI Installer – da primeira vez que se executa o MSI Installer, este ficheiro irá corrigir o sistema e criar um ficheiro de auditoria com a hora de conclusão.

Executar novamente o MSI Installer irá apresentar uma opção **Repair** (Reparar). O utilizador tem a opção de aplicar novamente o patch ou não. Nota: a não aplicação do patch resulta numa configuração insegura do instrumento.

Aplicar o patch de segurança do Local Run Manager

Para instalar o patch:

1. Inicie sessão no sistema com uma conta de administrador (p. ex., sbsadmin).

   A Illumina recomenda que a aplicação do patch se realize quando o instrumento não esteja em funcionamento. Caso o instrumento esteja a executar um ensaio, o patch deve ser aplicado imediatamente após a conclusão do mesmo.

2. Localize o patch transferido para o sistema.
3. Mova o ficheiro de instalação do patch para a pasta `C:\Illumina` (isenta da Política de restrição de software).
4. Faça duplo clique no ícone do ficheiro de instalação para lançar a interface.
5. Quando a aplicação carregar, selecione **Next** (Seguinte) para iniciar a instalação do patch.
6. No ecrã Installation Completion (Conclusão da instalação), selecione **Finish** (Terminar).

Caso seja necessário um relatório de verificação da instalação, consulte *Verificação* na página 5 (Verificação).

É necessário reiniciar o sistema no fim da instalação.

Reparação

Caso ocorra um erro, o cliente pode executar a reparação da instalação seguindo as instruções abaixo:

1. Inicie sessão no sistema com uma conta de administrador (p. ex., sbsadmin).
2. Localize o patch transferido para o sistema.
3. Mova o ficheiro de instalação do patch para a pasta `C:\Illumina` (isenta da Política de restrição de software).
4. Faça duplo clique no ícone do ficheiro de instalação para lançar a interface.
5. O ficheiro de instalação irá detetar automaticamente se a ferramenta de configuração foi executada antes e representa novas opções:
   a. Change (Alterar): sombreada a cinzento e não disponível.
   b. Repair (Reparar): repara erros e dá opções para reconfiguração.
   c. Remove (Remover): desinstala o patch e repõe a configuração predefinida (consulte *Desinstalação* na página 5).
6. No ecrã Installation Completion (Conclusão da instalação), selecione **Finish** (Terminar).

Caso seja necessário um relatório de verificação da instalação, consulte *Verificação* na página 5 (Verificação).

É necessário reiniciar o sistema no fim da instalação.

Desinstalação

A desinstalação do patch reverte as modificações efetuadas ao ficheiro de configuração anfitrião da aplicação.

1. Inicie sessão no sistema com uma conta de administrador (por ex., sbsadmin).
2. Localize o patch transferido para o sistema.
3. Mova o ficheiro de instalação do patch para a pasta `C:\Illumina` (isenta da Política de restrição de software).
4. Faça duplo clique no ícone do ficheiro de instalação para lançar a interface.
5. Selecione **Remove** (Remover) para desinstalar o patch e reverter todos os valores para as predefinições.
6. Selecione **Remove** (Remover) para verificar a opção de desinstalar o patch e reverter todos os valores para as predefinições.

Esta definição torna o sistema inseguro e vulnerável a ataques. Recomendamos vivamente a verificação de qualquer impacto técnico que a remoção do patch possa originar antes de optar pela desinstalação.

7. No ecrã Installation Completion (Conclusão da instalação), selecione **Finish** (Terminar).

Caso seja necessário um relatório de verificação da instalação, consulte *Verificação* na página 5 (Verificação).

Recomenda-se reiniciar o sistema no fim da instalação.

Verificação

Se houver necessidade de verificar a instalação, terá sido gerado um ficheiro de verificação que inclui um carimbo de data e hora, a versão do Local Run Manager instalada e outros valores de verificação chave. Para obter este ficheiro, contacte techsupport@illumina.com.

Recomendações adicionais de mitigação e segurança

A implementação segura dos instrumentos RUO e dos dispositivos médicos Dx depende de camadas de segurança. A Illumina recomenda vivamente a implementação dos instrumentos e dispositivos no contexto mais restrito de sub-rede ou segurança, com dispositivos de confiança. Recomenda-se vivamente a utilização de firewalls e outras políticas de rede para restringir outros acessos de entrada e saída.

Também recomendamos o seguinte:

- Ative a Transport Layer Security (TLS) para assegurar que todas as comunicações fora do instrumento são encriptadas.
  - Para ativar a Transport Layer Security (TLS), consulte o Local Run Manager Software Guide (Guia do software do Local Run Manager).

Opções alternativas

Se por algum motivo não for possível executar o patch, os seguintes métodos manuais de mitigação reduzem o risco:

- Desative o acesso remoto ao Local Run Manager adicionando regras de firewall do Windows para bloquear as ligações às portas 80 e 443.
  O MSI Installer irá bloquear automaticamente as ligações de entrada remotas na configuração do servidor Web do Local Run Manager. Uma mitigação manual que atinge o mesmo resultado é implementar uma configuração da firewall do Windows para bloquear ligações de entrada a ligações `HTTP (TCP:80)` e `HTTPS (TLS, TCP:443)`.
  Uma vez implementado, só é possível aceder ao Local Run Manager no computador em que o Local Run Manager está instalado; deixa de estar acessível a partir de outros computadores ligados à mesma rede.

> Se o fluxo de trabalho do utilizador implicar o acesso remoto ao Local Run Manager, esta funcionalidade deixa de estar disponível.

- Minimize o número de outros dispositivos na rede.
  Configurar a rede para minimizar o número de outros dispositivos na rede que podem comunicar com o instrumento afetado irá reduzir o risco de aproveitamento indevido. Quanto menos ligações estiverem disponíveis no sistema, menos oportunidades estarão disponíveis para acesso.
  Para tal pode ser necessário consultar os recursos de TI ou Segurança de informações.
- Remova o instrumento da rede.
  Caso nenhuma outra opção seja viável, a mitigação final é remover por completo o instrumento da rede. Esta ação irá desativar o acesso a serviços Illumina Cloud/SaaS, como o Proactive e o BaseSpace® Sequence Hub, e a fluxos de trabalho caraterísticos de descarga de dados genómicos.
  Para tal pode ser necessário consultar os recursos de TI ou Segurança de informações.

Investigação de possíveis acessos não autorizados

Os seguintes passos poderão auxiliar o operador do instrumento a determinar se um utilizador não autorizado acedeu ao sistema:

1. Verifique a existência de chamadas anormais nos registos dos IIS armazenados em `C:\inetpub\logs\LogFiles\W3SVC1`.
   - As chamadas normais ao servidor Web do Local Run Manager aparecem como se segue:
     ```
     GET http /normalresource.extension?normal-URI-decoration
     ```
   - As chamadas anormais ao servidor Web do Local Run Manager poderão aparecer, por exemplo, como se segue:
     ```
     POST http /hackertool.asp
     ```
2. Examine o registo dos IIS para procurar por sinais de carregamentos POST de conteúdos que não sejam ficheiros de manifesto. Por exemplo, as chamadas que se seguem indicariam uma atividade suspeita:
   ```
   wscript
   shell
   wscript.network
   scripting.filesystemObject
   ```
3. Se uma aplicação antivírus/antimalware estiver instalada, verifique os registos do software para detetar sinais de comportamento anormal.
4. Examine os registos do Windows para procurar sinais de mensagens de erro anormais.
   Se um ator de ameaça conseguisse acesso com direitos de administrador, teria a capacidade de alterar ou apagar todos os registos e eventos de instrumentos locais.

Verificar quaisquer pontos finais aos quais o sistema possa ter tentado aceder. Para uma lista das ligações de saída previstas, consulte Control Computer Firewall (Firewall do computador de controlo).

Conforme necessário, contacte o Suporte Técnico da Illumina para obter assistência.

Histórico de revisões

Documento	Data	Descrição da alteração
Documento n.º 200017330 v02	Abril de 2022	Adicionou-se uma recomendação para aplicar o patch quando o instrumento não está em funcionamento. Adicionou-se a instrução de que é necessário reiniciar o instrumento após a instalação do patch. Corrigiu-se a descrição do histórico de revisão da v01.
Documento n.º 200017330 v01	Abril de 2022	O título do documento foi alterado para Guia de instruções do patch de software do LRM 1.0. Todas as referências à v1.0.1 foram removidas. Adicionou-se uma secção sobre a investigação de possíveis acessos não autorizados.
Documento n.º 200017330 v00	Março de 2022	Edição inicial.