LRM Software Patch 1.0

illumina®

적용 가이드

소개

Illumina®는 Local Run Manager 소프트웨어의 보안 취약점을 발견하였으며, 이를 이용한 원격 공격으로부터 소프트웨어를 보호할 수 있는 패치(patch)를 제공하고자 합니다.

Local Run Manager는 독립형 소프트웨어 앱으로, 다음과 같은 시퀀싱 시스템의 기본 구성에 포함되어 있습니다.

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

*체외진단의료기기

본 가이드는 상기 명시된 Illumina 기기와 기기 외부 컴퓨터에 설치되어 있는 독립형 버전의 Local Run Manager에 적용됩니다.

이번에 발견된 취약점은 인증되지 않은 원격 명령어 실행(Remote Command Execution, RCE)이며, 완화 조치를 취하지 않을 경우 CVSS 점수는 10.0점(`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H`)으로 치명적(Critical)인 수준입니다.

상기 명시된 기기의 경우 다음과 같은 취약점 완화 조치를 취하시어 인가되지 않은 사용자가 한 대 이상의 기기에 접속하여 원격 접속 공격을 시도할 가능성으로부터 기기를 보호하시기 바랍니다.

어떤 이유로 패치 Installer의 실행이 불가능한 경우 본 문서의 후반부에 기술되어 있는 '추가적인 완화 조치 및 보안 권장 사항' 섹션을 참고하시거나 기술지원팀(techsupport@illumina.com)에 지원을 요청해 주시기 바랍니다.

패치의 복사본을 다운로드하거나 요청하는 방법은 Local Run Manager Security Patch 받기 섹션을 참고해 주시기 바랍니다.

- **v1.0.0 패치** – Local Run Manager 웹 구성을 업데이트하고 원격 인터넷 정보 서비스(Internet Information Services, IIS) 접속을 제한하는 패치

체외진단의료기기입니다.

연구 전용입니다. 진단 절차에는 사용할 수 없습니다.

Local Run Manager Security Patch 받기

Local Run Manager Security Patch를 받는 방법에는 네 가지가 있습니다.

방법1 – 기기에 직접 다운로드하기

가장 신속하게 Local Run Manager Security Patch를 받는 방법은 보안 패치 Installer를 호스팅 웹사이트에서 기기로 직접 다운로드하는 것입니다.

1. 보안 메일을 통해 제공된 링크를 클릭해 패치 Installer를 기기에 다운로드합니다.
2. 파일을 기기의 `C:\Illumina` 폴더로 옮깁니다.
3. 3페이지의 *Local Run Manager Security Patch 적용하기* 섹션의 지침을 따릅니다.

방법 2 – 패치 Installer를 컴퓨터에 다운로드한 후 USB 드라이브/공유 폴더를 통해 기기에 전송하기

보안 패치를 기기에 다운로드할 수 없는 경우 패치를 다른 컴퓨터에 우선 다운로드한 후 기기로 전송하는 방법을 권장합니다.

USB 드라이브는 사용 전 보안 담당자를 통해 무결성을 확인하시기 바랍니다(권장 사항).

1. 보안 메일을 통해 제공된 링크를 클릭하여 패치 Installer를 컴퓨터나 노트북에 다운로드합니다.
2. 다운로드한 패치 Installer를 USB 드라이브 또는 기기 내 공유 폴더로 복사합니다.
3. USB 드라이브를 사용하는 경우 기기에 연결합니다.
4. USB 드라이브 또는 공유 폴더에 들어 있는 패치 Installer를 기기의 `C:\Illumina` 폴더로 복사합니다.
5. 3페이지의 *Local Run Manager Security Patch 적용하기* 섹션의 지침을 따릅니다.

방법 3 – 기술지원팀에 지원 요청하기

Illumina의 기술지원팀이 다음 중 하나의 방법을 통해 패치 적용 과정을 안내해 드립니다.

- 기술지원팀의 원격 로그인

  기술지원팀이 원격으로 분석 기기에 접속하여 고객 대신 패치를 설치합니다.

  이 경우 반드시 원격으로 시스템에 접속이 가능해야 합니다.
  자세한 정보는 시설의 IT 담당자에게 문의해 주시기 바랍니다.

- 기술지원팀의 안내 지침

  기술지원팀이 유선을 통해 안내 지침을 제공하고, 시설의 IT 담당자로부터 기술 지원을 받으실 수 있습니다.

방법 4 – Illumina에 사전 구성된 드라이브 주문하기

쓰기 금지되어 있는 USB 드라이브를 무료로 주문 가능합니다. 패치가 설치된 USB 드라이브 주문 방법은 기술지원팀(techsupport@illumina.com)에 문의해 주시기 바랍니다.

선적 지연의 발생이나 재고 상황에 따라 일정에 맞춘 USB 드라이브 배송이 어려울 수 있습니다. 보다 신속하게 시스템을 보호하기 위해 가장 효율적인 방법을 선택하시기를 적극 권장해 드립니다.

Local Run Manager Security Patch v.1.0 Installer 적용하기

Illumina MSI(Microsoft Installer)는 실행 시 Local Run Manager 웹 서버의 구성을 업데이트하여 사용자가 업로드한 콘텐츠의 실행을 방지하고 LAN 네트워크 연결을 통한 Local Run Manager 웹 인터페이스 원격 접속을 차단합니다.

원격으로 기기에 접속하기 위해 Local Run Manager 웹 인터페이스를 사용하는 경우 패치를 설치하면 기존의 워크플로우가 더 이상 기능하지 못하게 됩니다. Illumina는 차후 이러한 이슈를 해결할 수 있는 영구적인 소프트웨어 수정을 통해 해당 기능을 복원할 계획입니다. 이러한 이슈로 인해 현재 구축되어 있는 워크플로우가 중단될 경우 기술지원팀(techsupport@illumina.com)에 지원을 요청하시기 바랍니다.

MSI는 모든 Local Run Manager 버전에 적용이 가능하며, 현재 기기/컴퓨터에 설치되어 있는 Local Run Manager의 버전에 적합한 수정을 자동으로 선택합니다.

또한 MSI는 성공적인 설치 여부를 확인할 수 있도록 타임스탬프와 완화 작업의 기록이 포함되어 있는 감사(audit) 파일을 생성합니다.

MSI는 최초 실행 시 시스템에 패치를 적용한 후 작업 완료 시간이 명시된 감사 파일을 생성합니다.

MSI를 다시 실행할 경우 **Repair** 옵션이 제공됩니다. 사용자는 이 옵션을 통해 패치를 다시 적용(reapply)하거나 이전 상태로 복구(roll back)할 수 있습니다. 참고로 이전 상태로의 복구는 안전하지 못한 기기 구성을 초래할 수 있습니다.

Local Run Manager Security Patch 적용하기

패치 설치 방법

1. 관리자 계정(예: sbsadmin)으로 시스템에 로그인합니다.

   패치는 기기를 사용하지 않을 때 적용하는 것을 권장합니다. 이미 기기가 런(run)을 수행 중이라면 런이 종료된 직후에 패치를 적용하시기 바랍니다.

2. 시스템에 다운로드해 둔 패치를 찾아 선택합니다.
3. 패치 Installer를 `C:\Illumina` 폴더(소프트웨어 제한 정책(Software Restriction Policy, SRP)에서 제외)로 옮깁니다.
4. Installer 아이콘을 더블클릭하여 인터페이스를 실행합니다.
5. 앱이 로딩되면 **Next**를 클릭하여 패치 설치를 시작합니다.
6. Installation Completion 화면에서 **Finish**를 선택합니다.

설치 보고서의 검증이 필요할 경우 5페이지의 *검증* 섹션을 참조하시기 바랍니다.

설치 완료 후 재부팅이 필요합니다.

복구

오류 발생 시 사용자는 다음의 절차에 따라 설치 복구(repair)를 실행할 수 있습니다.

1. 관리자 계정(예: sbsadmin)으로 시스템에 로그인합니다.
2. 시스템에 다운로드해 둔 패치를 찾아 선택합니다.
3. 패치 Installer를 `C:\Illumina` 폴더(SRP에서 제외)로 옮깁니다.
4. Installer 아이콘을 더블클릭하여 인터페이스를 실행합니다.
5. Installer가 구성 도구(configuration tool)의 과거 실행 여부를 자동으로 감지한 후 다음과 같은 새로운 옵션을 제공합니다.
   a. Change: 회색 음영으로 표시. 선택할 수 없음.
   b. Repair: 오류 복구 후 재구성 옵션 제공.
   c. Remove: 패치 제거 후 기본 구성으로 복원 (4페이지의 *제거* 섹션 참조).
6. Installation Completion screen 화면에서 **Finish**를 선택합니다.

설치 보고서의 검증이 필요할 경우 5페이지의 *검증* 섹션을 참조하시기 바랍니다.

설치 완료 후 재부팅이 필요합니다.

제거

패치를 제거(uninstallation)하면 앱 호스트 구성 파일이 수정 이전 상태로 되돌아갑니다.

1. 관리자 계정(예: sbsadmin)으로 시스템에 로그인합니다.
2. 시스템에 다운로드해 둔 패치를 찾아 선택합니다.
3. 패치 Installer를 `C:\Illumina` 폴더(SRP에서 제외)로 옮깁니다.
4. Installer 아이콘을 더블클릭하여 인터페이스를 실행합니다.
5. **Remove**를 선택하여 패치를 제거하고 모든 값을 기본 설정값으로 복원합니다.
6. **Remove**를 선택하여 패치를 제거하고 모든 값을 기본 설정값으로 복원하는 옵션을 확인합니다.

⚠ 이 설정은 시스템을 안전하지 않은 상태로 만들어 시스템을 공격의 위험에 노출할 수 있습니다. 따라서 패치를 제거하기 전에 Remove 옵션을 초래하는 모든 기술적 영향을 해결하는 것을 적극 권장합니다.

7. Installation Completion 화면에서 **Finish**를 선택합니다.

ⓘ 설치 보고서의 검증이 필요할 경우 5페이지의 *검증* 섹션을 참조하시기 바랍니다.

ⓘ 설치 완료 후 재부팅이 필요합니다.

검증

설치의 검증이 필요한 경우 설치 완료 후 생성된 검증(verification) 파일을 참고할 수 있습니다. 이 파일에는 날짜, 타임스탬프, 설치된 Local Run Manager의 버전 그리고 기타 주요 검증값이 포함되어 있습니다. 검증 파일을 원하시면 기술지원팀(techsupport@illumina.com)에 요청해 주시기 바랍니다.

추가적인 완화 조치 및 보안 권장 사항

RUO 기기와 Dx 의료 기기의 안전한 배치는 보안 단계에 달려 있습니다. Illumina는 RUO 기기와 Dx 의료 기기를 신뢰할 수 있는 기기(trusted device)와 함께 최소한의 네트워크 서브넷(subnet) 또는 보안 컨텍스트(security context)에 배치하는 것을 강력하게 권장합니다. 또한 다른 인바운드(inbound) 및 아웃바운드(outbound) 접속을 제한하기 위해 방화벽 및 기타 네트워크 정책의 사용을 적극 권장합니다.

추가로 다음과 같은 방법을 권장해 드립니다.

- 기기 밖에서 이루어지는 모든 통신을 암호화(encryption)하기 위해 전송 계층 보안(Transport Layer Security, TLS) 프로토콜을 활성화합니다.
  - TLS를 활성화하는 방법은 Local Run Manager 소프트웨어 가이드를 참조하시기 바랍니다.

기타 옵션

어떤 이유로 패치 실행이 불가능한 경우 사용자는 다음과 같은 완화 조치를 수동으로 실행하여 위험을 줄일 수 있습니다.

- 80번 포트와 443번 포트에서 들어오는 연결을 차단하는 Windows 방화벽 규칙을 추가해 원격 Local Run Manager 접속을 제한합니다.

  MSI는 자동으로 Local Run Manager 웹 서버 구성에서 들어오는 원격 연결을 차단합니다. 동일한 효과를 제공하는 수동 완화 조치로는 Windows 방화벽을 구성하여 `HTTP(TCP:80)` 및 `HTTPS(TLS, TCP:443)`로 들어오는 연결을 차단하는 방법이 있습니다.

  방화벽이 구성되면 사용자는 오직 Local Run Manager가 설치된 컴퓨터에서만 Local Run Manager에 접속할 수 있으며, 동일한 네트워크에 연결된 다른 컴퓨터에서는 더 이상 Local Run Manager에 접속할 수 없습니다.

사용자의 워크플로우에 원격 Local Run Manager 접속이 포함되어 있다면 본 기능은 더 이상 작동하지 않게 됩니다.

- 다른 네트워크 장비의 수 최소화하기

  문제가 있는 기기와의 통신이 가능한 다른 네트워크 장비의 수를 최소화하여 네트워크를 구성하면 공격의 가능성이 줄어듭니다. 시스템에 연결된 장비의 수가 적어지면 접속의 기회도 그만큼 적어집니다.

  이 방법을 실제로 실행하기 위해서는 시설의 정보 보안 또는 IT 담당자의 도움이 필요할 수 있습니다.

- 네트워크에서 기기 제거하기

  어떤 옵션도 적용이 불가능한 경우 마지막으로 시도 가능한 완화 조치는 네트워크에서 기기를 완전히 제거하는 것입니다. 이 방법은 Proactive와 BaseSpace® Sequence Hub와 같은 Illumina의 Cloud/SaaS 서비스뿐만 아니라 일반적인 유전체 데이터 오프로딩 워크플로우에 대한 접속을 제한합니다.

  이 방법을 실제로 실행하기 위해서는 시설의 정보 보안 또는 IT 담당자의 도움이 필요할 수 있습니다.

비인가 접속 가능성 확인하기

기기 사용자는 다음의 절차에 따라 인가되지 않은 사용자의 시스템 접속 기록을 확인해 볼 수 있습니다.

1. `C:\inetpub\logs\LogFiles\W3SVC1`에 저장되어 있는 IIS 로그에 비정상적인 호출(call)이 있는지 확인합니다.
   - 정상적인 Local Run Manager 웹 서버 호출은 다음과 같습니다.

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

   - 비정상적인 Local Run Manager 웹 서버 호출이 발생할 수 있습니다. 그 예시는 다음과 같습니다.

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

2. IIS 로그에 매니페스트(manifest) 파일 이외의 콘텐츠를 POST 방식으로 업로드한 기록이 있는지 확인합니다. 예를 들어 다음과 같은 호출은 의심스러운 활동으로 간주됩니다.

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

3. 안티바이러스/안티멀웨어 앱이 설치되어 있다면 소프트웨어 로그에 비정상적인 활동 기록이 있는지 확인해 보시기 바랍니다.
4. Windows 로그에 비정상적인 오류 메시지가 있는지 확인합니다.
   관리자 권한으로 접속에 성공한 위협 행위자는 모든 로컬 기기 로그와 이벤트를 변경하거나 삭제할 수 있게 됩니다.

마지막으로 시스템에서 접속을 시도한 엔드포인트(endpoint)가 있는지 확인합니다. 예상되는 아웃바운드 연결의 목록은 Control Computer Firewall 페이지를 참고하시기 바랍니다.

이와 관련해 도움이 필요하시면 Illumina 기술지원팀에 지원을 요청해 주시기 바랍니다.

개정 이력

문서	날짜	개정 내용
문서 번호: 200017330 v02	2022년 4월	기기가 작동 중이지 않을 때 패치를 적용할 것을 권장하는 내용 추가. 패치 설치 후 기기 재부팅이 필요하다는 지침 추가. 개정 이력 중 v01의 개정 내용 수정.
문서 번호: 200017330 v01	2022년 4월	문서 제목을 LRM Software Patch 1.0 적용 가이드로 변경. v1.0.1 패치 관련 내용 삭제. '비인가 접속 가능성 확인하기' 섹션 추가.
문서 번호: 200017330 v00	2022년 3월	최초 발행.

체외진단의료기기입니다.

연구 전용입니다. 진단 절차에는 사용할 수 없습니다.