Vá Lỗi Phần Mềm LRM 1.0

illumina®

Hướng Dẫn

Giới thiệu

Illumina® đã phát hiện một lỗ hổng bảo mật trong phần mềm Local Run Manager và đã cung cấp một bản vá phần mềm nhằm bảo vệ tránh việc khai thác lỗ hổng này từ xa.

Local Run Manager là một ứng dụng phần mềm độc lập nằm trong cấu hình mặc định trên các hệ thống sau:

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

*Dùng cho chẩn đoán trong ống nghiệm.

Hướng dẫn này áp dụng cho các thiết bị của Illumina liệt kê ở trên và cho cả các máy tính ngoài thiết bị đã cài đặt phiên bản Local Run Manager độc lập.

Lỗ hổng này là một kỹ thuật Thực Thi Lệnh Từ Xa (RCE, Remote Command Execution) Không Được Xác Thực có mức điểm khi chưa giảm rủi ro là 10,0 (Nghiêm trọng) theo Hệ Thống Chấm Điểm Lỗ Hổng Phổ Biến (CVSS, Common Vulnerability Scoring System), `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H`.

Các bước giảm rủi ro sau đây là bắt buộc đối với những thiết bị liệt kê ở trên nhằm tránh nguy cơ người dùng trái phép truy cập vào một hoặc nhiều thiết bị và thực hiện cuộc tấn công truy cập từ xa.

Nếu vì lý do nào đó mà bạn không thể chạy trình cài đặt, hãy tham khảo phần về các biện pháp giảm rủi ro bổ sung ở cuối tài liệu này hoặc liên hệ với techsupport@illumina.com để được hỗ trợ thêm.

Xem phần Cách lấy Bản Cập Nhật Của Local Run Manager để biết các tùy chọn về cách tải về hoặc yêu cầu một bản sao của bản vá lỗi.

- **Bản vá lỗi v1.0.0**: Bản này sẽ cập nhật cấu hình web của Local Run Manager và vô hiệu hóa quyền truy cập Internet Information Services (IIS) từ xa.

Cách lấy Bản Vá Lỗi Bảo Mật Của Local Run Manager

Có bốn (4) tùy chọn để lấy Bản Vá Lỗi Bảo Mật Của Local Run Manager.

Tùy chọn 1: Trực tiếp tải về thiết bị của bạn

Cách nhanh nhất để lấy Bản Cập Nhật Bảo Mật Của Local Run Manager là trực tiếp tải từ trang web lưu trữ về thiết bị.

1. Truy cập vào liên kết được cung cấp thông qua email bảo mật rồi tải trình cài đặt bản vá lỗi về thiết bị.
2. Chuyển tệp vào thư mục `C:\Illumina` trên thiết bị.
3. Làm theo hướng dẫn tại phần *Áp dụng Bản Vá Lỗi Bảo Mật Của Local Run Manager* trên trang 3.

Tùy chọn 2: Tải trình cài đặt bản vá lỗi về máy tính rồi chuyển trình cài đặt này sang thiết bị thông qua ổ USB/thư mục dùng chung

Nếu bạn không tải được bản vá lỗi bảo mật xuống thiết bị, chúng tôi khuyến nghị bạn tải bản vá lỗi xuống một máy tính khác rồi chuyển sang thiết bị.

Hãy cùng các đại diện về Bảo Mật xác minh xem ổ USB có nguyên vẹn hay không trước khi sử dụng. (Khuyến nghị)

1. Truy cập vào liên kết được cung cấp thông qua email bảo mật rồi tải trình cài đặt bản vá lỗi về máy tính để bàn hoặc máy tính xách tay.
2. Sao chép trình cài đặt bản vá lỗi đã tải về máy tính vào ổ USB hoặc thư mục dùng chung.
3. Đối với ổ USB, hãy cắm ổ vào Thiết Bị.
4. Sao chép trình cài đặt bản vá lỗi từ ổ USB hoặc thư mục dùng chung vào thư mục `C:\Illumina` trên thiết bị.
5. Làm theo hướng dẫn tại phần *Áp dụng Bản Vá Lỗi Bảo Mật Của Local Run Manager* trên trang 3.

Tùy chọn 3: Yêu cầu Hỗ Trợ Kỹ Thuật

Đại diện Bộ Phận Hỗ Trợ Kỹ Thuật của Illumina sẽ hướng dẫn bạn về toàn bộ quá trình vá lỗi bằng một trong các phương thức sau:

- Bộ Phận Hỗ Trợ Kỹ Thuật đăng nhập từ xa
  Đại diện Bộ Phận Hỗ Trợ Kỹ Thuật sẽ truy cập từ xa vào thiết bị phân tích và cài đặt bản vá lỗi thay mặt cho khách hàng.

  Hệ thống phải cho phép truy cập từ xa. Nếu bạn có câu hỏi, hãy yêu cầu đại diện CNTT tại địa phương trợ giúp.

- Hướng Dẫn Từ Xa
  Đại diện Bộ Phận Hỗ Trợ Kỹ Thuật sẽ hướng dẫn từ xa qua điện thoại. Vui lòng liên hệ với đại diện Bộ Phận Hỗ Trợ Kỹ Thuật tại địa phương để được trợ giúp.

Tùy chọn 4: Đặt mua ổ đã định cấu hình sẵn từ Illumina

Khách hàng có thể đặt mua ổ USB chống ghi mà không mất phí. Để đặt mua ổ đã được cài đặt bản vá lỗi, vui lòng liên hệ với techsupport@illumina.com.

Hoạt động gửi hàng hoặc nhập hàng tồn kho có thể bị chậm trễ, làm ảnh hưởng đến việc giao hàng đúng thời hạn. Để bảo vệ hệ thống một cách kịp thời hơn, chúng tôi đặc biệt khuyến nghị khách hàng bảo vệ hệ thống bằng phương thức đưa ra hướng giải quyết hiệu quả nhất.

Áp dụng Trình Cài Đặt Bản Vá Lỗi Bảo Mật Local Run Manager v.1.0

MSI (Microsoft Installer) của Illumina, khi được thực thi, sẽ cập nhật cấu hình máy chủ web của Local Run Manager để ngăn việc thực thi bất cứ nội dung nào do người dùng tải lên và chặn mọi quyền truy cập từ xa vào giao diện web của Local Run Manager qua kết nối Mạng Máy Tính Cục Bộ (LAN, Local Area Network).

Đối với người dùng sử dụng giao diện web của Local Run Manager để truy cập từ xa vào thiết bị, quy trình công việc này sẽ ngừng hoạt động sau khi bản vá lỗi v.1.0 được cài đặt. Illumina dự định sẽ khôi phục chức năng này sau bằng bản sửa lỗi phần mềm cố định dành cho sự cố này. Nếu việc này làm gián đoạn các quy trình công việc đã thiết lập, vui lòng liên hệ với techsupport@illumina.com để được hỗ trợ thêm.

Trình cài đặt MSI áp dụng cho mọi phiên bản Local Run Manager và sẽ tự động xác định bản sửa lỗi phù hợp dựa trên phiên bản Local Run Manager được cài đặt trên thiết bị/máy tính.

Trình cài đặt MSI cũng sẽ tạo một tệp kiểm tra cho thấy biện pháp giảm rủi ro này đã được thực hiện cùng với dấu thời gian để phản ánh quy trình cài đặt thích hợp.

Chạy Trình Cài Đặt MSI – trong lần chạy đầu tiên, Trình Cài Đặt MSI sẽ vá lỗi cho hệ thống và tạo một tệp kiểm tra ghi rõ thời gian hoàn thành.

Nếu bạn cho chạy lại Trình Cài Đặt MSI thì tùy chọn **Repair** (Sửa lỗi) sẽ xuất hiện, người dùng có thể áp dụng lại hoặc rút lại bản vá lỗi. Lưu ý: Việc rút lại bản vá lỗi sẽ dẫn đến cấu hình thiết bị không an toàn.

Áp dụng Bản Vá Lỗi Bảo Mật Của Local Run Manager

Cách cài đặt bản vá lỗi:

1. Đăng nhập vào hệ thống qua tài khoản quản trị viên (ví dụ như sbsadmin).

Illumina khuyến nghị áp dụng bản vá lỗi khi thiết bị không chạy. Nếu thiết bị đang chạy, nên áp dụng bản vá lỗi ngay sau khi chạy xong.

2. Tìm đến vị trí lưu bản vá lỗi mà bạn đã tải về hệ thống.
3. Chuyển trình cài đặt bản vá lỗi vào thư mục `C:\Illumina` (được miễn áp dụng Chính Sách Hạn Chế Phần Mềm).
4. Nhấp đúp vào biểu tượng trình cài đặt để khởi chạy giao diện.
5. Khi ứng dụng tải, chọn **Next** (Tiếp) để bắt đầu cài đặt bản vá lỗi.
6. Trên màn hình Installation Completion (Hoàn Tất Quá Trình Cài Đặt), chọn **Finish** (Hoàn tất).

Trong trường hợp cần xác minh báo cáo cài đặt, vui lòng xem phần *Xác minh* trên trang 5.

Bạn cần phải khởi động lại thiết bị khi kết thúc quá trình cài đặt.

Sửa lỗi

Trong trường hợp xảy ra lỗi, khách hàng có thể sửa lỗi cài đặt theo hướng dẫn sau:

1. Đăng nhập vào hệ thống qua tài khoản quản trị viên (ví dụ như sbsadmin).
2. Tìm đến vị trí lưu bản vá lỗi mà bạn đã tải về hệ thống.
3. Chuyển trình cài đặt bản vá lỗi vào thư mục `C:\Illumina` (được miễn áp dụng Chính Sách Hạn Chế Phần Mềm).
4. Nhấp đúp vào biểu tượng trình cài đặt để khởi chạy giao diện.
5. Trình cài đặt sẽ tự động phát hiện xem công cụ cấu hình đã được thực thi trước đó chưa và đưa ra các tùy chọn mới:
   a. Change (Thay đổi): Chuyển sang màu xám và không dùng được
   b. Repair (Sửa lỗi): Sửa lỗi và đưa ra các tùy chọn định lại cấu hình.
   c. Remove (Gỡ bỏ): Gỡ cài đặt bản vá lỗi và khôi phục về cấu hình mặc định (xem phần *Gỡ cài đặt* trên trang 4)
6. Trên màn hình Installation Completion (Hoàn Tất Quá Trình Cài Đặt), chọn **Finish** (Hoàn tất).

Trong trường hợp cần xác minh báo cáo cài đặt, vui lòng xem phần *Xác minh* trên trang 5.

Bạn cần phải khởi động lại thiết bị khi kết thúc quá trình cài đặt.

Gỡ cài đặt

Nếu bạn gỡ cài đặt bản vá lỗi, những nội dung sửa đổi đã được thực hiện đối với tệp cấu hình máy chủ ứng dụng sẽ bị hủy bỏ.

1. Đăng nhập vào hệ thống qua tài khoản quản trị viên (ví dụ như sbsadmin).
2. Tìm đến vị trí lưu bản vá lỗi mà bạn đã tải về hệ thống.
3. Chuyển trình cài đặt bản vá lỗi vào thư mục `C:\Illumina` (được miễn áp dụng Chính Sách Hạn Chế Phần Mềm).
4. Nhấp đúp vào biểu tượng trình cài đặt để khởi chạy giao diện.

5. Chọn **Remove** (Gỡ bỏ) để gỡ cài đặt bản vá lỗi và khôi phục mọi giá trị về chế độ cài đặt mặc định.
6. Chọn **Remove** (Gỡ bỏ) để xác minh tùy chọn gỡ cài đặt bản vá lỗi và khôi phục mọi giá trị về chế độ cài đặt mặc định.

⚠ Chế độ cài đặt này sẽ khiến hệ thống rơi vào trạng thái không an toàn và có nguy cơ bị tấn công. Chúng tôi đặc biệt khuyến nghị rằng trước khi chọn gỡ cài đặt bản vá lỗi, bạn hãy giải quyết mọi tác động về mặt kỹ thuật dẫn đến tùy chọn này.

7. Trên màn hình Installation Completion (Hoàn Tất Quá Trình Cài Đặt), chọn **Finish** (Hoàn tất).

ℹ Trong trường hợp cần xác minh báo cáo cài đặt, vui lòng xem phần *Xác minh* trên trang 5.

ℹ Bạn nên khởi động lại thiết bị khi kết thúc quá trình cài đặt.

Xác minh

Nếu cần xác minh việc cài đặt, hệ thống sẽ tạo một tệp xác minh có ngày và dấu thời gian, phiên bản Local Run Manager được cài đặt và các giá trị xác minh quan trọng khác. Để lấy tệp này, vui lòng liên hệ với techsupport@illumina.com.

Khuyến Nghị Bổ Sung Về Bảo Mật và Giảm Rủi Ro

Việc triển khai an toàn các thiết bị Chỉ Dùng Cho Mục Đích Nghiên Cứu (RUO, Research Use Only) và thiết bị y tế Chẩn Đoán (Dx, Diagnosis) phụ thuộc vào các lớp bảo mật. Illumina đặc biệt khuyến nghị bạn triển khai các thiết bị trong mạng con hoặc bối cảnh bảo mật mạng nhỏ nhất, cùng với các thiết bị đáng tin cậy. Chúng tôi cũng rất khuyến khích việc sử dụng tường lửa và các chính sách mạng khác để hạn chế quyền truy cập vào và ra khác.

Chúng tôi cũng khuyến nghị:

- Bật Giao Thức Bảo Mật Tầng Truyền Tải (TLS, Transport Layer Security) để đảm bảo mọi dữ liệu truyền tải qua lại ngoài thiết bị đều được mã hóa.
  - Để bật giao thức Bảo Mật Tầng Truyền Tải (TLS), vui lòng tham khảo Hướng Dẫn về Phần Mềm Local Run Manager.

Các Tùy Chọn Thay Thế

Nếu vì lý do nào đó mà bạn không thể thực hiện việc vá lỗi, các phương pháp thủ công sau đây sẽ giúp giảm rủi ro:

- Vô hiệu hóa quyền truy cập từ xa vào Local Run Manager bằng cách thêm các quy tắc tường lửa của Windows để chặn kết nối đến ở Cổng 80 và 443.

Trình Cài Đặt MSI sẽ tự động chặn các kết nối đến từ xa trong cấu hình máy chủ web của Local Run Manager. Biện pháp giảm rủi ro thủ công sau cũng cho hiệu quả tương tự: Triển khai cấu hình tường lửa của Windows để chặn các kết nối đến `HTTP (TCP:80)` và kết nối `HTTPS (TLS, TCP:443)`.
Sau khi triển khai, bạn chỉ có thể truy cập vào Local Run Manager trên máy tính đã cài đặt Local Run Manager chứ không thể truy cập từ các máy tính khác kết nối với cùng một mạng được nữa.

Nếu quy trình công việc yêu cầu người dùng truy cập từ xa vào Local Run Manager, thì chức năng này sẽ không còn hiệu quả nữa.

- Giảm thiểu số lượng thiết bị mạng khác.
  Việc định cấu hình mạng để giảm thiểu số lượng những thiết bị mạng khác có thể giao tiếp với thiết bị chịu ảnh hưởng sẽ giúp giảm nguy cơ khai khác. Càng ít thiết bị có thể kết nối với hệ thống thì cơ hội truy cập sẽ càng ít.
  Bạn có thể cần trao đổi với các nguồn lực CNTT hoặc Bảo Mật Thông Tin ở địa phương để thực hiện giải pháp này.
- Xóa thiết bị khỏi mạng.
  Nếu không còn phương án khả thi nào khác, biện pháp giảm rủi ro cuối cùng là xóa hẳn thiết bị khỏi mạng. Cách làm này sẽ vô hiệu hóa quyền truy cập vào các dịch vụ Đám Mây/Phần Mềm dưới dạng Dịch Vụ (SaaS, Software as a Service) của Illumina như Proactive và BaseSpace® Sequence Hub, cũng như các quy trình công việc giảm tải dữ liệu bộ gen điển hình.
  Bạn có thể cần trao đổi với các nguồn lực CNTT hoặc Bảo Mật Thông Tin ở địa phương để thực hiện giải pháp này.

Điều Tra Nguy Cơ Truy Cập Trái Phép

Các bước sau đây có thể hỗ trợ người vận hành thiết bị xác định xem có người dùng trái phép truy cập vào hệ thống hay không:

1. Kiểm tra nhật ký IIS lưu trữ tại `C:\inetpub\logs\LogFiles\W3SVC1` để phát hiện lệnh gọi bất thường.
   - Lệnh gọi bình thường đến máy chủ web của Local Run Manager sẽ hiện lên như sau:
     ```
     GET http /normalresource.extension?normal-URI-decoration
     ```
   - Lệnh gọi bất thường đến máy chủ web của Local Run Manager có thể hiện lên như trong ví dụ sau:
     ```
     POST http /hackertool.asp
     ```
2. Kiểm tra nhật ký IIS để tìm dấu hiệu của các lệnh POST tải lên nội dung không phải là tệp phiếu kê khai. Ví dụ: các lệnh gọi sau đây thể hiện hoạt động đáng ngờ:
   ```
   wscript
   shell
   wscript.network
   ```

```
scripting.filesystemObject
```

3. Nếu bạn đã cài đặt ứng dụng chống vi-rút/chống phần mềm độc hại, hãy kiểm tra nhật ký phần mềm để tìm dấu hiệu của hành vi bất thường.
4. Kiểm tra nhật ký Windows để tìm dấu hiệu của thông báo lỗi bất thường.
   Nếu một tác nhân đe dọa giành được quyền truy cập của quản trị viên, tác nhân đó sẽ có khả năng sửa đổi hoặc xóa toàn bộ nhật ký và sự kiện trong thiết bị cục bộ.

Kiểm tra mọi điểm cuối mà hệ thống có thể đã tìm cách truy cập. Để biết danh sách các kết nối đi dự kiến, hãy tham khảo phần Tường Lửa Của Máy Tính Điều Khiển.

Liên hệ với Bộ Phận Hỗ Trợ Kỹ Thuật của Illumina để nhận được sự trợ giúp cần thiết.

Lịch sử sửa đổi

Tài liệu	Ngày	Mô tả thay đổi
Tài liệu số 200017330 v02	Tháng 4 năm 2022	Bổ sung đề xuất áp dụng bản vá lỗi khi thiết bị không chạy. Bổ sung hướng dẫn về việc cần khởi động lại thiết bị sau khi cài đặt bản vá lỗi. Sửa phần mô tả lịch sử sửa đổi cho v01.
Tài liệu số 200017330 v01	Tháng 4 năm 2022	Sửa tiêu đề tài liệu thành Hướng Dẫn Vá Lỗi Phần Mềm LRM 1.0. Xóa mọi nội dung đề cập đến v1.0.1. Bổ sung phần đề cập đến việc điều tra nguy cơ truy cập trái phép.
Tài liệu số 200017330 v00	Tháng 3 năm 2022	Phát hành lần đầu.