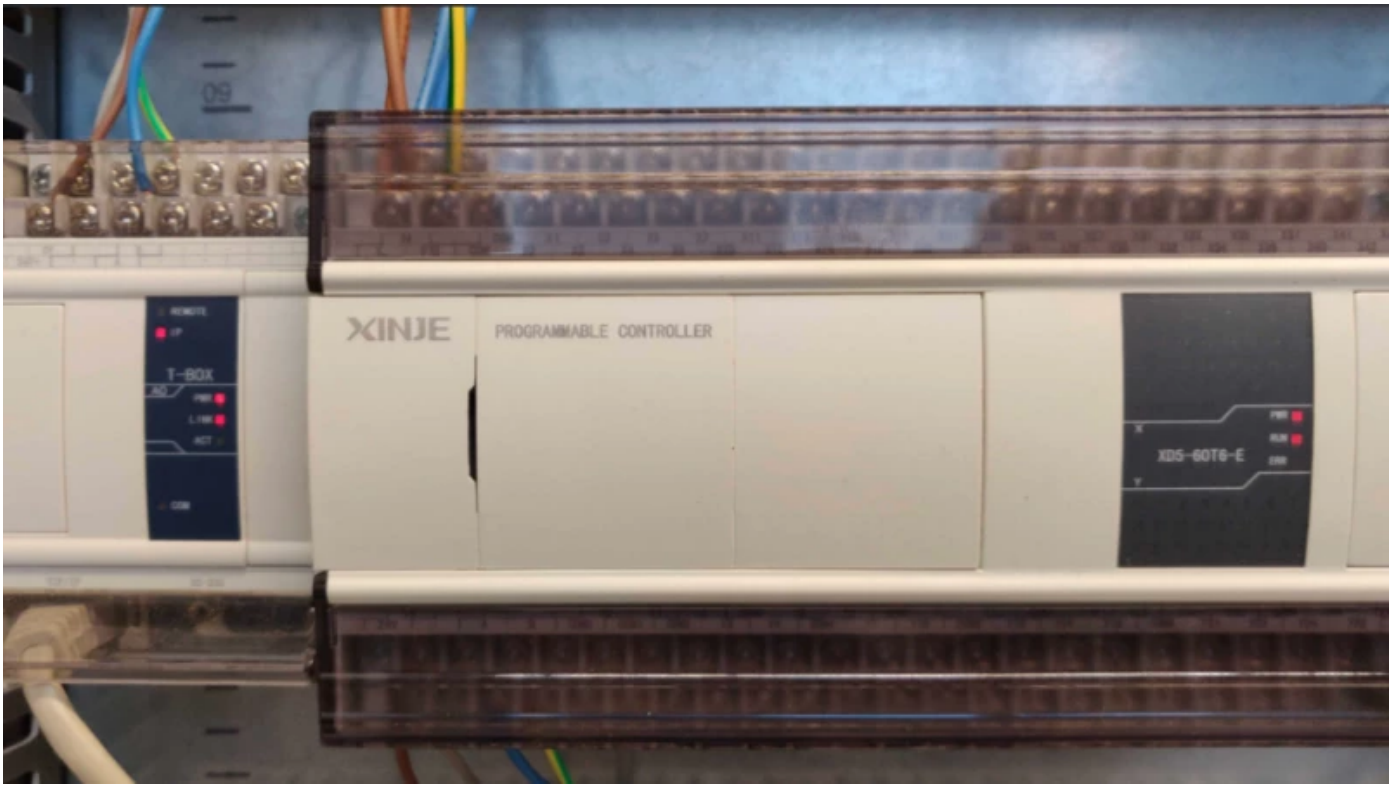
82

Nghiên cứu của Team82

Từ tệp dự án đến thực thi mã: Khai thác lỗ hổng trong Công cụ chương trình PLC XINJE

Mashav Sapir / Ngày 11 tháng 5 năm 2022



Tóm tắt điều hành

- Team82 đã phát hiện ra hai lỗ hổng trong Công cụ chương trình PLC của XINJE, một máy trạm kỹ thuật.
- Phiên bản 3.5.1 bị ảnh hưởng và có thể cả các phiên bản khác cũng bị ảnh hưởng.
- Team82 bắt đầu nỗ lực tiết lộ thông tin vào tháng 8 năm 2020. Hơn một năm sau, XINJE thừa nhận thông tin tiết lộ của chúng tôi vào tháng 9 năm 2021.
- XINJE lúc đó đã từ chối hợp tác với Team82 và yêu cầu chúng tôi ngừng liên lạc với họ.
- Chúng tôi đã mở rộng các điều khoản trong **chính sách phối hợp công bố thông tin** của mình từ 90 ngày đến 9 tháng trước khi tiết lộ một số chi tiết hạn chế vào hôm nay để giúp chủ sở hữu tài sản ưu tiên mọi biện pháp giảm nhẹ.
- Kẻ tấn công có thể sử dụng tệp dự án được tạo thủ công để kích hoạt các lỗ hổng này.
- Các tệp dự án tùy ý có thể được ghi vào tệp dự án để thực thi mã.

- CISA đã **đưa ra lời khuyên tại đây.**

Máy trạm kỹ thuật là một trong những tài sản công nghệ vận hành (OT) quan trọng nhất. Các kỹ sư sử dụng các nền tảng này để định cấu hình và duy trì các ứng dụng và thiết bị hệ thống điều khiển ở cấp độ thấp hơn của Mô hình Purdue cho các hệ thống điều khiển công nghiệp. Một tác nhân đe dọa có thể truy cập và sử dụng máy trạm kỹ thuật làm vectơ tấn công có thể làm gián đoạn các quy trình công nghiệp và gây ra thiệt hại có thể gây nguy hiểm cho an toàn công cộng hoặc làm gián đoạn việc cung cấp các dịch vụ quan trọng.

Nghiên cứu mới nhất của Team82 là kiểm tra các ứng dụng máy trạm kỹ thuật được bán bởi **XINJE** , một công ty tự động hóa Trung Quốc. Chúng tôi đã phát hiện hai lỗ hổng trong Công cụ chương trình PLC XINJE (**CVE-2021-34605** và **CVE-2021-34606**) trong v3.5.1. Team82 chỉ thử nghiệm v3.5., chúng tôi tin rằng các phiên bản khác cũng có thể dễ bị tấn công.

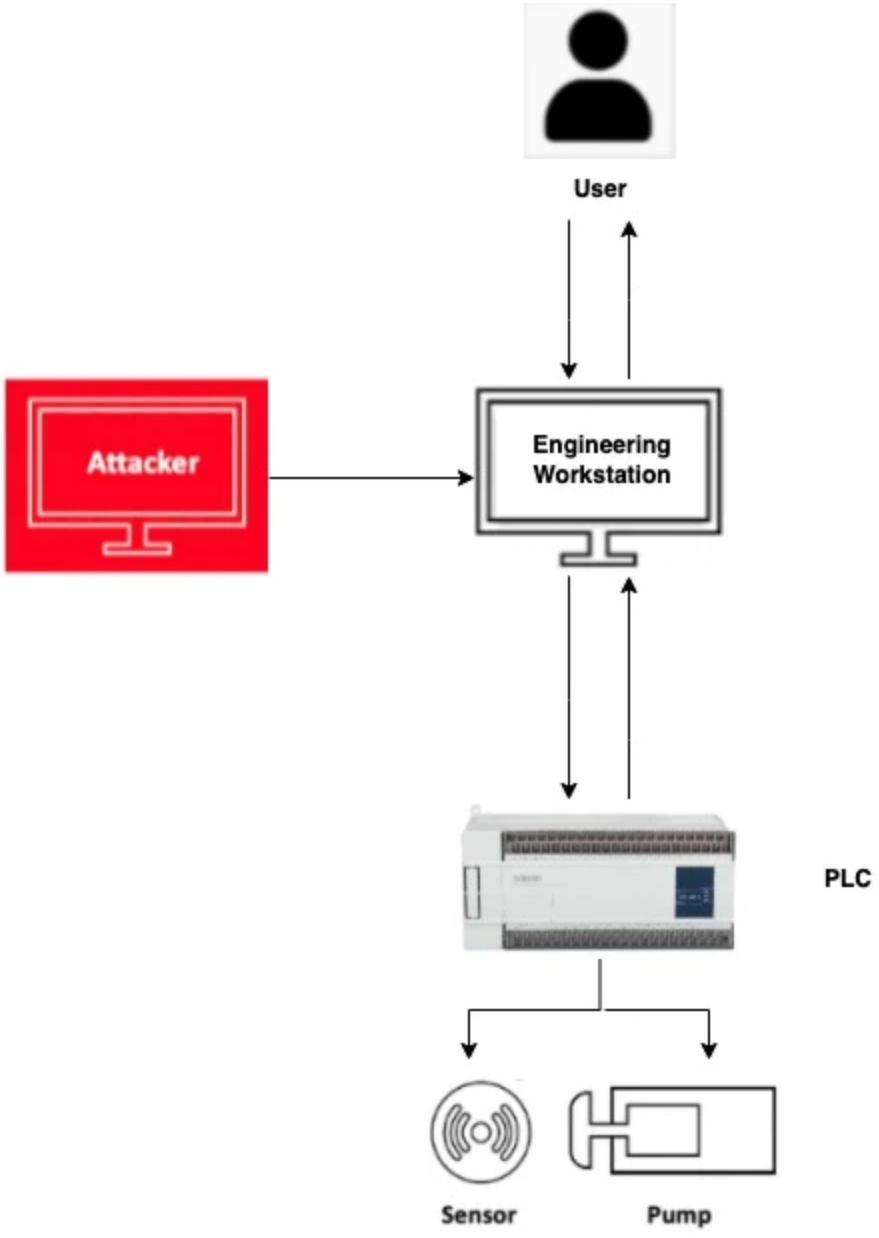
Những sai sót này có thể được kích hoạt bởi một tệp dự án được tạo thủ công. Kẻ tấn công có thể sử dụng các lỗ hổng này để ghi các tệp dự án tùy ý vào PLC và thực thi mã.

Hôm nay Team82 tiết lộ một số thông tin hạn chế về những lỗ hổng này, thông tin chi tiết về chúng đã được tiết lộ riêng tư vào cuối tháng 8 năm 2021 sau một năm cố gắng kết nối với đại diện của công ty. Nhà cung cấp không tiếp thu những nỗ lực của chúng tôi trong việc chia sẻ thông tin kỹ thuật cũng như cộng tác để khắc phục và phản hồi. Cuối cùng, vào ngày 8 tháng 9 năm 2021, đại diện XINJE đã yêu cầu Team82 ngừng liên lạc. Team82 đã gia hạn các điều khoản của chính sách phối hợp công bố thông tin từ 90 ngày đến 9 tháng trước khi tiết lộ một số thông tin chi tiết hạn chế vào hôm nay để giúp chủ sở hữu tài sản ưu tiên mọi biện pháp giảm nhẹ.

Chương trình máy trạm kỹ thuật

Công cụ chương trình PLC của XINJE là một chương trình máy trạm kỹ thuật, được sử dụng trong môi trường OT để giao tiếp với các PLC do XINJE sản xuất. Theo XINJE, những thiết bị này không chỉ được bán ở Trung Quốc mà còn ở Châu Âu, Bắc Mỹ, Đông Nam Á và các nơi khác ở một số thị trường, bao gồm năng lượng, sản xuất và kỹ thuật.

Từ góc độ bảo mật, việc giành quyền truy cập vào máy chứa chương trình máy trạm kỹ thuật có thể cho phép kẻ tấn công can thiệp hoàn toàn vào PLC và các thiết bị OT có độ nhạy cao khác với những hậu quả bất lợi. Do đó, việc khai thác lỗ hổng trong các ứng dụng này có thể bị kẻ tấn công lợi dụng như bước cuối cùng để chiếm toàn quyền kiểm soát mạng OT.



Kẻ tấn công nhắm mục tiêu vào máy trạm kỹ thuật có thể lây nhiễm sang các thiết bị cấp thấp hơn như PLC, cảm biến hoặc máy bơm.

Các tệp dự án độc hại nằm trong trung tâm của một loại lỗ hổng bảo mật

Team82 đặc biệt quan tâm đến một loại lỗ hổng liên quan đến các tệp dự án.

Tệp dự án thường là định dạng tệp lưu trữ có chứa tệp OLE, cơ sở dữ liệu SQLite, định dạng nhị phân độc quyền, tệp văn bản và thư mục được tạo trong các máy trạm kỹ thuật. Các chương trình này được các kỹ sư sử dụng để giám sát, cấu hình và giao tiếp với bộ điều khiển logic khả trình (PLC) và các hệ thống điều khiển khác.

Logic chương trình có trong tệp dự án chi phối các thiết bị ICS và giám sát các quy trình, đồng thời nó cũng có thể bao gồm dữ liệu cấu hình mạng và đôi khi là bố cục mạng OT hoàn chỉnh. Đối với những kẻ tấn công nhắm mục tiêu vào các mạng công nghiệp - và nhiều người trong số họ sau này là chủ thể nhà nước - các tệp dự án được vũ khí hóa có thể sẽ là trọng tâm của một chiến dịch như vậy.

Khi tệp dự án được mở bằng chương trình trạm kỹ thuật, chương trình có thể nhanh chóng liên lạc với các thiết bị liên quan. Ngoài ra, kỹ sư OT đôi khi có thể tải tệp dự án lên từ PLC, nhưng điều này yêu cầu chạy công cụ khám phá mạng để tìm địa chỉ mạng của PLC (một quy trình không được tất cả các PLC hỗ trợ) hoặc nhập thủ công các thông số mạng liên quan. Kết quả là nhiều công ty lựa chọn sử dụng các tệp dự án, mỗi tệp bao gồm cấu hình cho một hoặc nhiều PLC.

Các lỗ hổng có thể được kích hoạt bởi **các tệp dự án** được tạo ra đặc biệt do kẻ tấn công tạo ra khi chương trình trạm kỹ thuật mở. Ví dụ: trong trường hợp này, kẻ tấn công có thể thay thế một tệp hợp pháp trong chia sẻ mạng được sử dụng để lưu trữ các tệp bằng một tệp được tạo thủ công sẽ gây ra lỗ hổng trong chương trình. Chúng tôi đã phát hiện ra các lỗ hổng như vậy trong Công cụ chương trình PLC XINJE. Công cụ này có thể cho phép kẻ tấn công chạy mã tùy ý trên điểm cuối dễ bị tấn công khi mở tệp dự án bị khai thác.

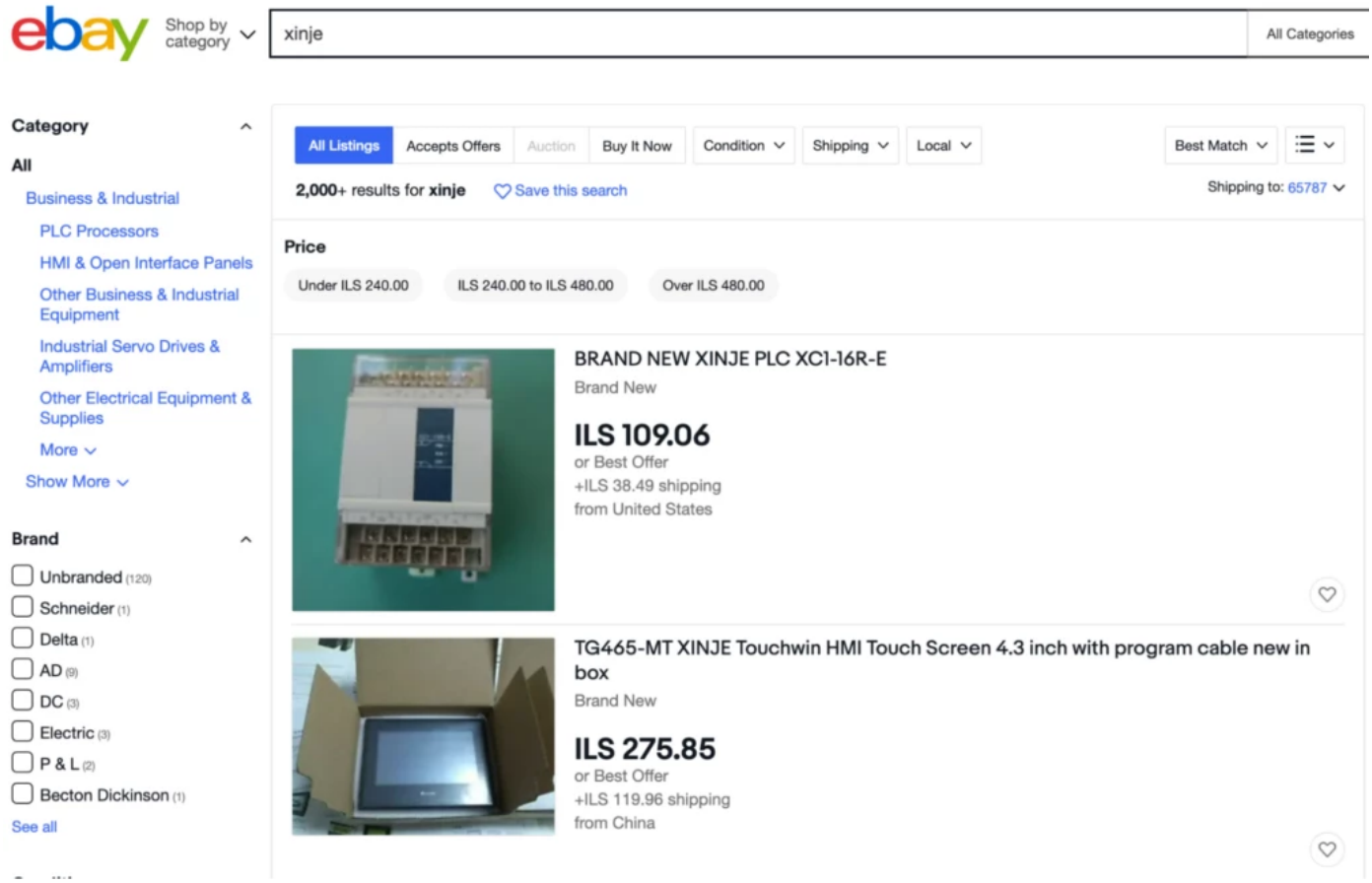
Thiết lập môi trường nghiên cứu Bước quan trọng đầu tiên

Là một phần công việc của chúng tôi, chúng tôi thường nhận được yêu cầu nghiên cứu các giao thức độc quyền nhằm tối đa hóa khả năng quan sát lưu lượng truy cập trong mạng của khách hàng. Đôi khi, chúng tôi phải hỗ trợ các thiết bị cũ hơn vẫn được sử dụng với những vai trò quan trọng tại địa điểm sản xuất và đôi khi, chúng tôi thậm chí còn vấp phải thiết bị do các nhà cung cấp OT nhỏ hơn sản xuất.

Yêu cầu mà chúng tôi nhận được từ khách hàng về việc phân tích các giao thức được sử dụng bởi thiết bị do XINJE sản xuất thuộc loại sau.

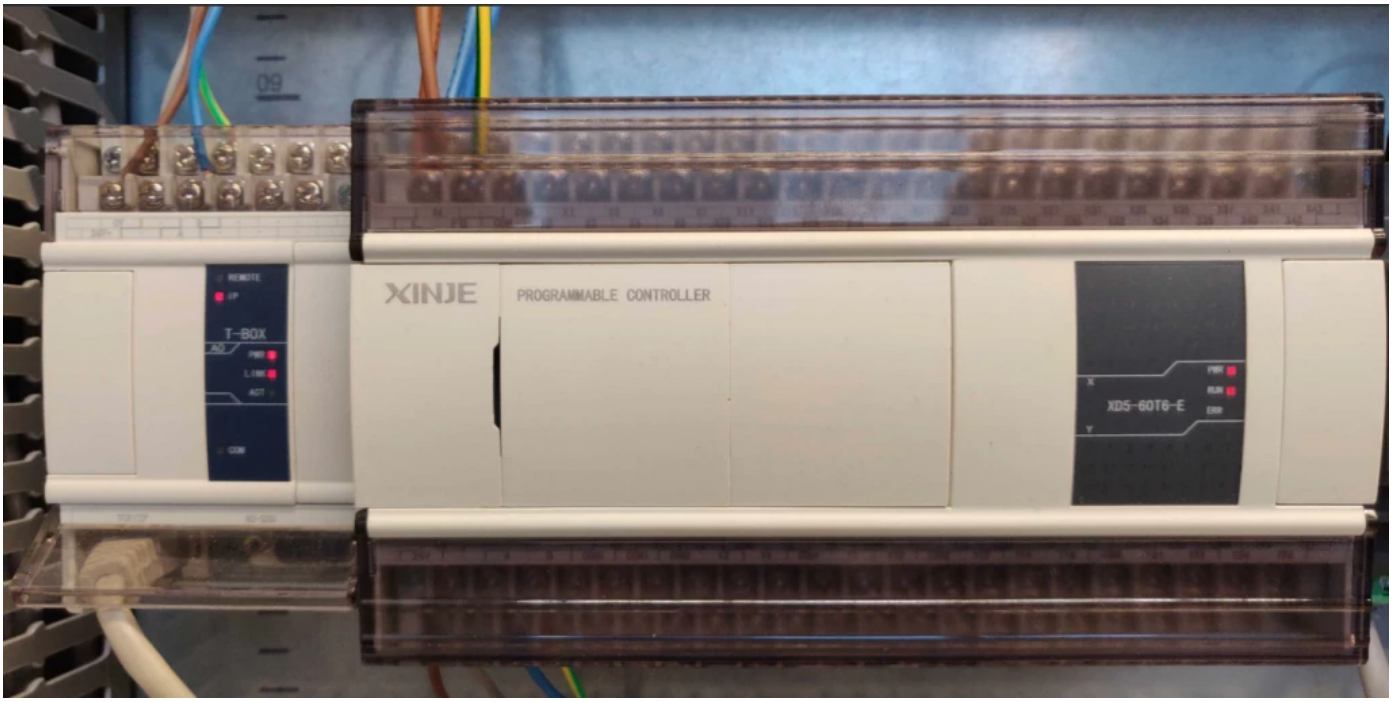
Bước đầu tiên của chúng tôi là tạo một phòng thí nghiệm; điều này thường yêu cầu mua thiết bị và kết nối nó với chương trình máy trạm kỹ thuật có liên quan. Trong một số trường hợp, ngay cả việc mua thiết bị cũng có thể gặp khó khăn vì nhà cung cấp có thể không còn cung cấp đúng mẫu mã mà chúng tôi cần.

Những gì chúng tôi phát hiện ra theo thời gian là có thể mua được nhiều loại thiết bị OT thông qua eBay. Trong nhiều trường hợp, khi một nhà máy thay đổi thiết bị OT, thiết bị cũ hơn đã qua sử dụng sẽ xuất hiện trên eBay và có thể được mua dễ dàng và vận chuyển đến tận nhà bạn. Thiết bị do XINJE cung cấp cũng không ngoại lệ và bạn có thể mua nhiều loại sản phẩm XINJE qua eBay:



Danh sách eBay cho thiết bị công nghiệp XINJE.

Sau khi chúng tôi mua PLC, bước tiếp theo là cài đặt nó trong phòng thí nghiệm của chúng tôi, cùng với vô số thiết bị OT khác và kết nối nó với chương trình máy trạm kỹ thuật được sử dụng để cấu hình nó.



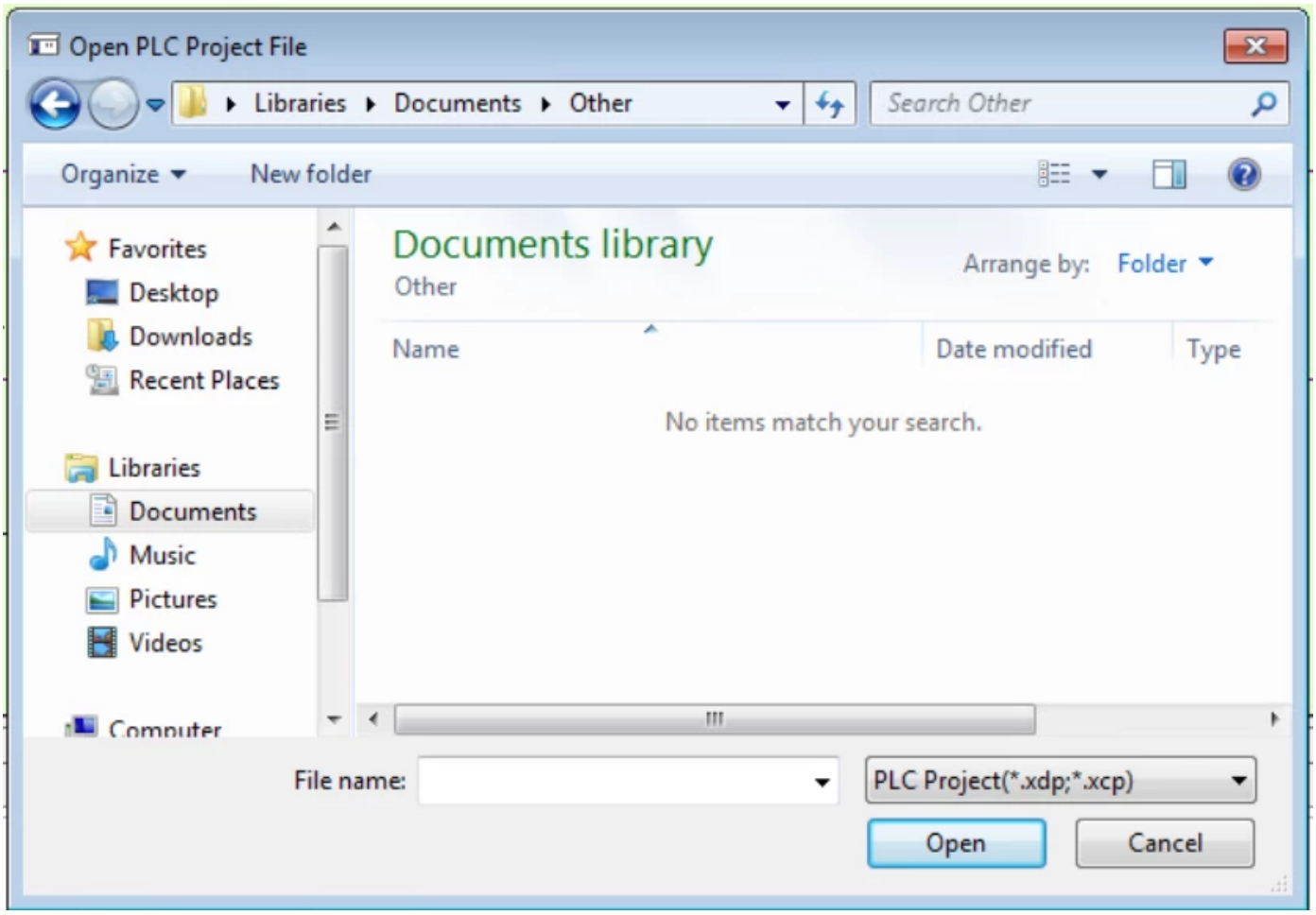
Một PLC XINJE đang chạy trong phòng thí nghiệm.

Liên kết hai lỗ hổng để tải một tệp độc hại

Sau khi chúng tôi đã xây dựng một thiết lập phù hợp và hoàn tất việc nghiên cứu các giao thức khác nhau mà thiết bị sử dụng, chúng tôi thường được khách hàng yêu cầu tìm kiếm các vấn đề bảo mật với thiết lập.

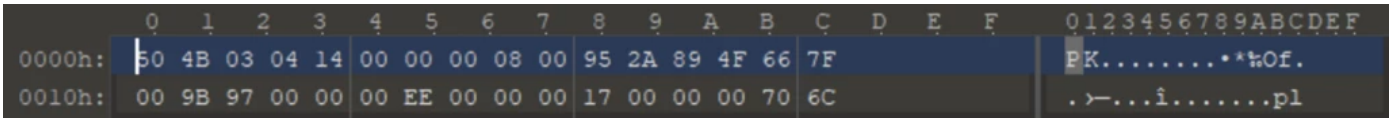
Việc chỉ ra những vấn đề này có thể giúp người dùng cải thiện tình trạng bảo mật của họ ngay lập tức. Việc báo cáo một cách có trách nhiệm các lỗ hổng này cho nhà cung cấp có thể giúp khắc phục chúng và cải thiện tính bảo mật trên toàn bộ không gian OT.

Trong trường hợp của XINJE, chúng tôi quyết định tập trung vào chương trình máy trạm kỹ thuật có tên là Công cụ chương trình PLC XINJE. Như đã đề cập trước đó, trong những trường hợp như vậy, các lỗ hổng trong tệp dự án được đặc biệt quan tâm. Thông thường, việc tìm kiếm lỗ hổng tệp dự án bắt đầu bằng việc điều tra cấu trúc của tệp dự án được chương trình máy trạm kỹ thuật sử dụng. Trong trường hợp Công cụ chương trình PLC XINJE, các tệp có liên quan là các tệp *.xdp:



Cấu trúc tệp dự án PLC XINJE là tệp .xdp.

Các tệp dự án này có thể dễ dàng được xác định là tệp zip, như được biểu thị bằng phép thuật PK\x03\x04 bên dưới:



Và chúng có thể được giải nén bằng hầu hết mọi tiện ích lưu trữ (ví dụ: 7z). Điều thú vị hơn nữa là khi chương trình mở một tệp dự án, nó sẽ ngay lập tức trích xuất nó vào một thư mục tạm thời nằm trong thư mục cài đặt của nó:

Time of Day	Process Name	PID	Operation	Path	Result
11:27:09.5810642 AM	XDPPro.exe	784	WriteFile	C:\Program Files\XINJE\XDPPro\tmp\Save\FuncBlock	SUCCESS
11:27:09.6845469 AM	XDPPro.exe	784	WriteFile	C:\Program Files\XINJE\XDPPro\tmp\Save\ipdevices.xmd	SUCCESS
11:27:09.6850059 AM	XDPPro.exe	784	WriteFile	C:\Program Files\XINJE\XDPPro\tmp\Save\prjinfo.xmd	SUCCESS
11:27:09.6853103 AM	XDPPro.exe	784	WriteFile	C:\Program Files\XINJE\XDPPro\tmp\Save\xjinfo.data	SUCCESS
11:27:09.6891928 AM	XDPPro.exe	784	WriteFile	C:\Program Files\XINJE\XDPPro\tmp\Save\funcblock\func1.fcb	SUCCESS
11:27:09.6895720 AM	XDPPro.exe	784	WriteFile	C:\Program Files\XINJE\XDPPro\tmp\Save\funcblock\xcp.fcblst	SUCCESS
11:27:09.6911269 AM	XDPPro.exe	784	WriteFile	C:\Program Files\XINJE\XDPPro\tmp\Save\plc1\configfunclist.xmd	SUCCESS

XDPPro.exe ghi một số tệp vào C:\Program Files\XINJE\XDPPro\tmp

Hành vi này cho biết rằng chương trình giả định rằng nó đang được thực thi với đặc quyền của quản trị viên. Điều này, kết hợp với việc tệp được trích xuất là tệp zip, ngay lập tức khiến người ta tự hỏi liệu lỗ hổng trượt zip (lỗ hổng ghi đè tệp tùy ý) có thể được lợi dụng để có được đặc quyền ghi tùy ý hay không.

Chẳng bao lâu sau, chúng tôi đã tìm thấy lỗ hổng zip slip (**CVE-2021-34605**), lỗ hổng này có thể cung cấp cho kẻ tấn công đặc quyền ghi tùy ý với các quyền của chương trình; trong hầu hết các trường hợp đây sẽ là đặc quyền của quản trị viên.

Câu hỏi tiếp theo là làm cách nào để thực thi mã từ việc ghi tệp tùy ý. Vì việc mã được thực thi ngay sau khi tệp dự án được tải là hợp lý nhất nên chúng ta có thể kiểm tra xem chương trình đang làm gì trong khi mở tệp dự án:

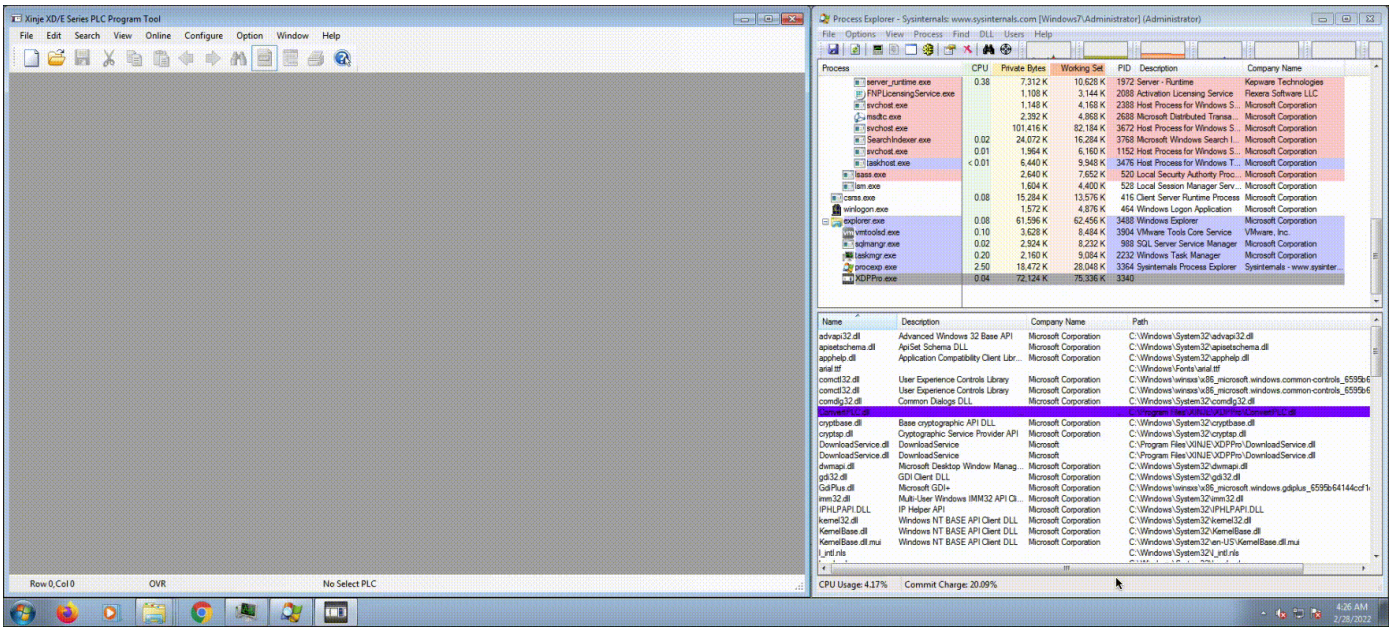
11:27:10.2837666 AM	XDPPro.exe	784	CreateFile	C:\Program Files\XINJE\XDPPro\DNSAPI.dll	NAME NOT FOUND
11:27:10.2839065 AM	XDPPro.exe	784	CreateFile	C:\Windows\System32\dnsapi.dll	SUCCESS
11:27:10.2839770 AM	XDPPro.exe	784	QueryBasic...	C:\Windows\System32\dnsapi.dll	SUCCESS
11:27:10.2839843 AM	XDPPro.exe	784	CloseFile	C:\Windows\System32\dnsapi.dll	SUCCESS
11:27:10.2841152 AM	XDPPro.exe	784	CreateFile	C:\Windows\System32\dnsapi.dll	SUCCESS
11:27:10.2842318 AM	XDPPro.exe	784	CreateFile...	C:\Windows\System32\dnsapi.dll	FILE LOCKED WITH
11:27:10.2842635 AM	XDPPro.exe	784	CreateFile...	C:\Windows\System32\dnsapi.dll	SUCCESS
11:27:10.2843855 AM	XDPPro.exe	784	Load Image	C:\Windows\System32\dnsapi.dll	SUCCESS

XDPPro.exe cố tải DNSAPI.dll từ C:\Program Files\XINJE\XDPPro, không tìm thấy nó và quay lại C:\Windows\System32

Điều thú vị là nó đang cố tải các tệp .dll từ thư mục cục bộ của nó bằng LoadLibrary. Khi LoadLibrary không tìm thấy chúng, nó sẽ quay lại tìm kiếm chúng trong C:\Windows\System32. Đây là nơi chúng tôi tìm thấy lỗ hổng thứ hai, **CVE-2021-34606** , một lỗ hổng tấn công DLL cổ điển.

Để tạo ra một cách khai thác hoạt động hoàn chỉnh, chúng tôi đã liên kết hai lỗ hổng của mình: Sau khi XINJE PLC Program Tool mở tệp dự án độc hại được tạo đặc biệt, lỗ hổng zip slip sẽ được kích hoạt và tệp .dll sẽ được ghi vào thư mục của chương trình trong Tệp chương trình. Sau này trong quá trình tải một dự án mới, DLL này sẽ được tải thay vì DLL thực (nằm trong Windows\System32).

Sau khi DLL được tải, mã độc sẽ được thực thi trong quy trình DLLMain của nó hoặc trong một trong các chức năng được chương trình nhập vào. Kẻ tấn công bây giờ có thể có được chỗ đứng trên mạng OT.



Trình diễn cách khai thác bằng chứng khái niệm của Team82.

Kết thúc công cụ chương trình PLC XINJE

Mặc dù thực tế là nhận thức về an ninh mạng đã tăng lên đều đặn trong những năm gần đây trong thế giới OT, nhiều chương trình máy trạm kỹ thuật vẫn dễ bị tấn công bởi các lỗ hổng dễ bị khai thác.

Không phải tất cả các nhà cung cấp đều nhận thức được thực tế rằng các tệp dự án có thể bị kẻ tấn công lợi dụng như một phương pháp để chiếm quyền kiểm soát các tài nguyên OT quan trọng; điều này cũng đúng với hầu hết nhân viên OT.

Ngoài ra, nhiều nhà cung cấp vẫn chưa có giao diện rõ ràng để phối hợp tiết lộ các lỗ hổng. Do đó, việc tiết lộ có thể mất một thời gian dài không cần thiết, thường được chuyển qua các nhóm bán hàng và/hoặc hỗ trợ kỹ thuật mà không có kiến thức về bảo mật, trước khi đến được với các nhóm chịu trách nhiệm phát triển các sản phẩm bị ảnh hưởng.

Đây là một tiết lộ đầy thách thức với XINJE, rất may đây không phải là tiêu chuẩn ở phần lớn các nhà cung cấp OT.

Chia sẻ:

Tiết lộ lỗ hổng gần đây

CVE-2023-41741

Việc lộ thông tin nhạy cảm trước lỗ hổng tác nhân trái phép trong thành phần cgi trong Trình quản lý bộ định tuyến Synology (SRM) trước 1.3.1-9346-6 cho phép kẻ tấn công từ xa lấy được thông tin nhạy cảm thông qua các vectơ không xác định.

Lỗ hổng này cho phép kẻ tấn công từ xa tiết lộ thông tin nhạy cảm trên các bản cài đặt bị ảnh hưởng của bộ định tuyến Synology RT6600ax. Không cần xác thực để khai thác lỗ hổng này.

Lỗ hổng cụ thể tồn tại trong tệp info.cgi. Sự cố xảy ra do dữ liệu nhạy cảm bị lộ trên giao diện WAN. Kẻ tấn công có thể lợi dụng lỗ hổng này để tiết lộ một số thông tin nhất định trong bối cảnh của quy trình hiện tại.

CVSS V3: 5.3

CVE-2023-41740

Việc giới hạn không đúng tên đường dẫn đến lỗ hổng thư mục bị hạn chế ('Path Traversal') trong thành phần cgi trong Trình quản lý bộ định tuyến Synology (SRM) trước 1.3.1-9346-6 cho phép kẻ tấn công từ xa đọc các tệp cụ thể thông qua các vectơ không xác định.

Lỗ hổng này cho phép kẻ tấn công lân cận mạng tiết lộ thông tin nhạy cảm trên các bản cài đặt bộ định tuyến Synology RT6600ax bị ảnh hưởng. Không cần xác thực để khai thác lỗ hổng này.

Lỗ hổng cụ thể tồn tại trong tệp uistrings.cgi. Sự cố xảy ra do thiếu xác thực thích hợp đường dẫn do người dùng cung cấp trước khi sử dụng nó trong các thao tác tệp. Kẻ tấn công có thể lợi dụng lỗ hổng này để tiết lộ

thông tin trong bối cảnh của quy trình hiện tại.

CVSS V3: 5.3

CVE-2023-41738

Việc vô hiệu hóa không đúng cách các thành phần đặc biệt được sử dụng trong lỗ hổng lệnh hệ điều hành ('OS Command Insert') trong Chức năng miền thư mục trong Trình quản lý bộ định tuyến Synology (SRM) trước 1.3.1-9346-6 cho phép người dùng được xác thực từ xa thực thi các lệnh tùy ý thông qua các vectơ không xác định.

Lỗ hổng này cho phép kẻ tấn công lân cận mạng thực thi mã tùy ý trên các bản cài đặt bị ảnh hưởng của bộ định tuyến Synology RT6600ax. Cần phải xác thực để khai thác lỗ hổng này.

Lỗ hổng cụ thể tồn tại trong điểm cuối API WEB. Sự cố xảy ra do thiếu xác thực thích hợp chuỗi do người dùng cung cấp trước khi sử dụng chuỗi đó để thực hiện lệnh gọi hệ thống. Kẻ tấn công có thể lợi dụng lỗ hổng này để thực thi mã trong ngữ cảnh root.

CVSS V3: 7.2

CVE-2023-41739

Lỗ hổng tiêu thụ tài nguyên không được kiểm soát trong Chức năng tệp trong Trình quản lý bộ định tuyến Synology (SRM) trước 1.3.1-9346-6 cho phép người dùng được xác thực từ xa thực hiện các cuộc tấn công từ chối dịch vụ thông qua các vectơ không xác định.

Lỗ hổng này cho phép những kẻ tấn công lân cận mạng tạo điều kiện từ chối dịch vụ đối với các bản cài đặt bị ảnh hưởng của bộ định tuyến Synology RT6600ax. Cần phải xác thực để khai thác lỗ hổng này.

Lỗ hổng cụ thể tồn tại trong tệp SYNO.Core. Sự cố xảy ra do việc tiêu thụ tài nguyên không được kiểm soát. Kẻ tấn công có thể lợi dụng lỗ hổng này để tạo điều kiện từ chối dịch vụ trên thiết bị.

CVSS V3: 4.9

CVE-2023-39227

CWE-256: Lưu trữ bản rõ của mật khẩu

Sản phẩm bị ảnh hưởng lưu trữ tên người dùng và mật khẩu ở dạng văn bản gốc. Việc lưu trữ văn bản gốc có thể bị kẻ tấn công lạm dụng để rò rỉ thông tin xác thực hợp pháp của người dùng.

Softneta khuyến nghị người dùng nên cập nhật lên v7.2.9.820 của MedDream PACS Server hoặc vá hệ thống hiện tại của họ bằng Fix-v230712.

CVSS V3: 6.1

CÁC GIẢI PHÁP

An ninh mạng công nghiệp

An ninh mạng chăm sóc sức khỏe

An ninh mạng thương mại

An ninh mạng khu vực công

NGHIÊN CỨU MỐI ĐE DỌA

Trang chủ Team82

Trang tổng quan tiết lộ lỗ hổng bảo mật

Nghiên cứu

Khóa PGP

ĐỐI TÁC

Đối tác

Đối tác liên minh công nghệ

Đối tác kênh

Nhà cung cấp dịch vụ bảo mật được quản lý

Trở thành đối tác

Tìm một người bạn đồng hành

Đăng nhập đối tác

TÀI NGUYÊN

Thư viện tài nguyên

Blog

Giấy trắng

Báo cáo

Nghiên cứu điển hình

Bảng dữ liệu

Tóm tắt hội nhập

Podcast

Video

CÔNG TY

Về chúng tôi

Nghề nghiệp

Khả năng lãnh đạo

Phòng tin tức

Trung tâm Tin tưởng

Sự kiện

Liên hệ chúng tôi