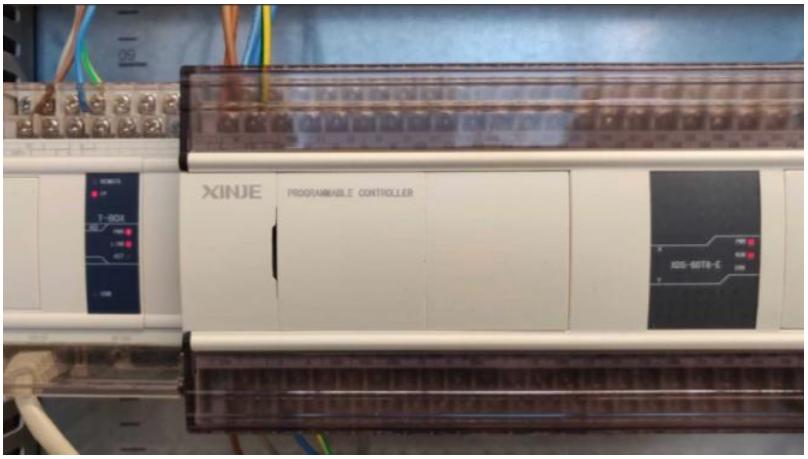
Team82 Research

From Project File to Code Execution: Exploiting Vulnerabilities in XINJE PLC Program Tool

Mashav Sapir / May 11th, 2022



Executive Summary

- Team82 has uncovered two vulnerabilities in XINJE's PLC Program Tool, an engineering workstation.
- Version 3.5.1 is affected, and likely other versions.
- Team82 began disclosure efforts in August 2020. More than a year later, XINJE acknowledged our disclosure in September 2021.
- XINJE at that time refused to cooperate with Team82 and asked us to stop communication with them.
- We extended the terms of our **coordinated disclosure policy** beyond 90 days to nine months before disclosing limited details today to help asset owners prioritize any mitigations.
- An attacker may use a crafted project file to trigger these vulnerabilities.
- Arbitrary project files may be written to a project file to gain code execution.

Engineering workstations are among the most critical operational technology (OT) assets. Engineers use these platforms to configure and maintain control system applications and devices at lower levels of the Purdue Model for industrial control systems. A threat actor who can access and use an engineering workstation as an attack vector is in position to disrupt industrial processes and cause damage that could put public safety at risk or interrupt the delivery of critical services.

Team82's latest research is an examination of engineering workstation applications sold by **XINJE**, a Chinese automation company. We uncovered two vulnerabilities in the XINJE PLC Program Tool (**CVE-2021-34605** and **CVE-2021-34606**) in v3.5.1. Team82 tested only v3.5., we believe other versions may be vulnerable too.

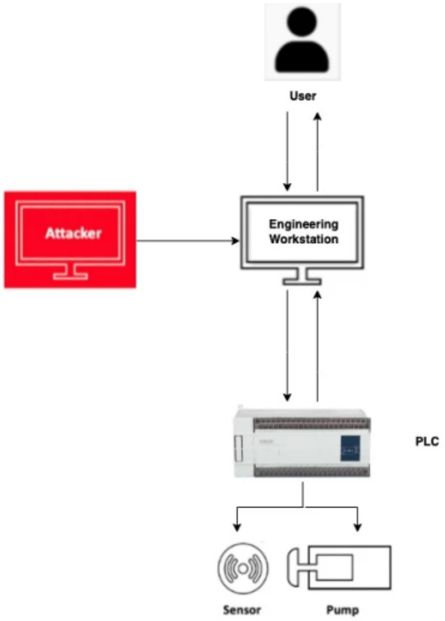
These flaws can be triggered by a crafted project file. An attacker can use these vulnerabilities to write arbitrary project files to a PLC and gain code execution.

Team82 is disclosing limited information today about these vulnerabilities, details of which were privately disclosed at the end of August 2021 after a year of attempting to connect with representatives of the company. The vendor was not receptive to our attempts to share technical information and collaborate on a fix and response. Finally, on Sept. 8, 2021, XINJE representatives asked that Team82 stop communication. Team82 extended the terms of its coordinated disclosure policy beyond 90 days to nine months before disclosing limited details today to help asset owners prioritize any mitigations.

Engineering Workstation Programs

n OT environments to communicate with XINJE-produced PLCs. These devices, according to XINJE, are sold not only in China, but also in Europe, North America, Southeast Asia, and elsewhere in a number of markets, including energy, manufacturing, and engineering.

From a security perspective, gaining access to a machine containing the engineering workstation program can allow an attacker to fully meddle with PLCs and other highly sensitive OT equipment with adverse consequences. Therefore, exploiting vulnerabilities in these applications can be used by attackers as a final step toward taking full control of an OT network.



An attacker targeting an engineering workstation could infect lower-level devices such as PLCs, sensors, or pumps.

Malicious Project Files at Heart of a Class of Vulnerabilities

Team82 has taken a special interest in a class of vulnerabilities that involve project files.

Project files are usually archive file formats that contain OLE files, SQLite databases, proprietary binary formats, text files, and directories created within engineering workstations. These programs are used by engineers to monitor, configure, and communicate with programmable logic controllers (PLCs) and other control systems.

The program logic contained in a project file governs ICS devices and oversees processes, and it also may include network configuration data and—at times—a complete OT network layout. For attackers targeting industrial networks—and many of late have been state actors—weaponized project files would likely be central to such a campaign.

When a project file is opened with an engineering station program, the program can quickly communicate with the relevant equipment. Alternatively, the OT engineer can sometimes upload the project file from a PLC, but this requires either running a network discovery tool to find the PLC's network address (a procedure not supported by all PLCs) or manually entering the relevant network parameters. As a result, many companies opt to use project files, each including the configuration for one or more PLCs.

Vulnerabilities can be triggered by specially crafted project files composed by an attacker when opened by the engineering station program. In this scenario, an attacker could, for example, replace a legitimate file in a network share used to store the files with a crafted file that would trigger a vulnerability in the program. We discovered such vulnerabilities in the XINJE PLC Program Tool, which can allow an attacker to run arbitrary code on a vulnerable endpoint upon opening an exploited project file.

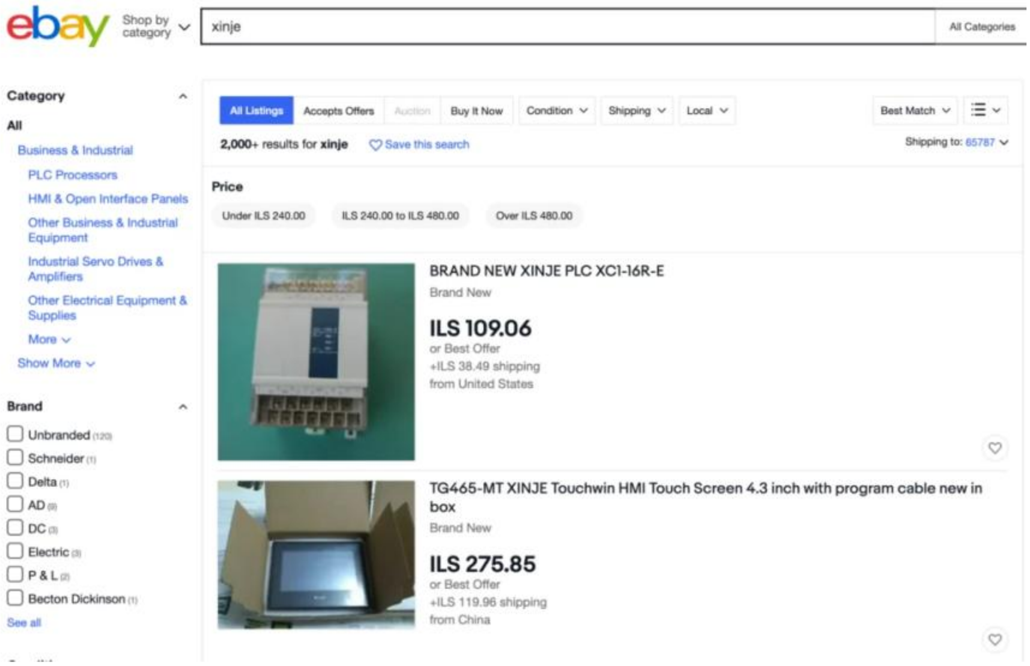
Research Environment Setup a Crucial First Step

As part of our work, we often receive requests to research proprietary protocols in order to maximize our customers' ability to observe the traffic in their network. At times we have to support older equipment still used in critical roles in production sites, and at other times we even stumble onto equipment manufactured by smaller OT vendors.

The request we received from a customer to analyze protocols used by equipment manufactured by XINJE fell into the latter category.

Our first step was to create a lab setup; this usually requires purchasing equipment and connecting it to the relevant engineering workstation program. In some cases, even purchasing the equipment can be difficult because the vendor might no longer offer the exact models we need.

What we discovered over time is that a surprisingly wide range of OT equipment can be purchased through eBay. In many cases, once a factory changes its OT equipment, the older, used equipment winds up on eBay and can be purchased easily and shipped to your doorstep. Equipment offered by XINJE was no exception, and a variety of XINJE products can be purchased through eBay:



Category
All
Business & Industrial
PLC Processors
HMI & Open Interface Panels
Other Business & Industrial Equipment
Industrial Servo Drives & Amplifiers
Other Electrical Equipment & Supplies
More
Show More

Brand
- □ Unbranded (120)
- □ Schneider (1)
- □ Delta (1)
- □ AD (8)
- □ DC (3)
- □ Electric (3)
- □ P & L (2)
- □ Becton Dickinson (1)

See all

2,000+ results for **xinje** Save this search

Shipping to: 65787

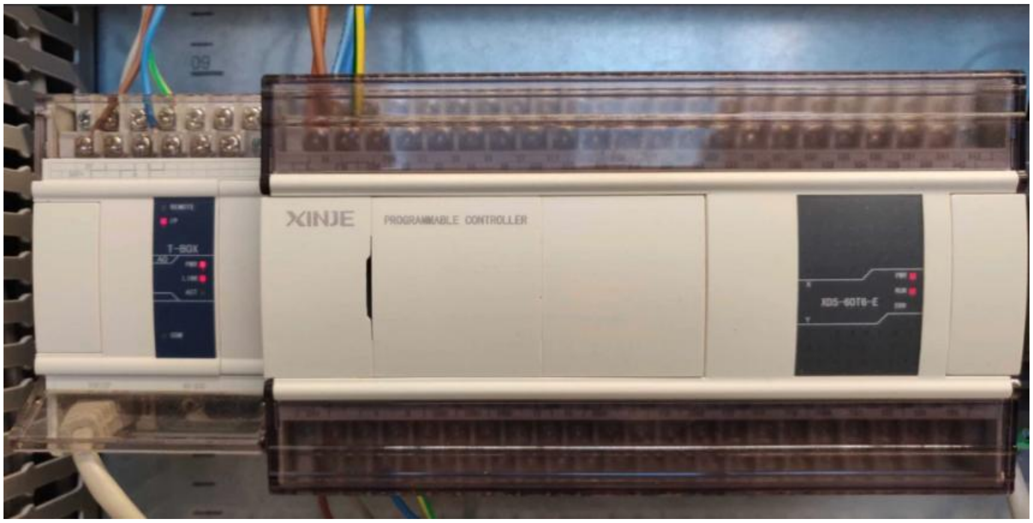
Price
Under ILS 240.00
ILS 240.00 to ILS 480.00
Over ILS 480.00

BRAND NEW XINJE PLC XC1-16R-E
Brand New
ILS 109.06
or Best Offer
+ILS 38.49 shipping
from United States

TG465-MT XINJE Touchwin HMI Touch Screen 4.3 inch with program cable new in box
Brand New
ILS 275.85
or Best Offer
+ILS 119.96 shipping
from China

EBay listings for XINJE industrial equipment.

Once we purchased a PLC, the next step was to install it in our lab, along with a multitude of other OT equipment, and connect it to the engineering workstation program used to configure it.



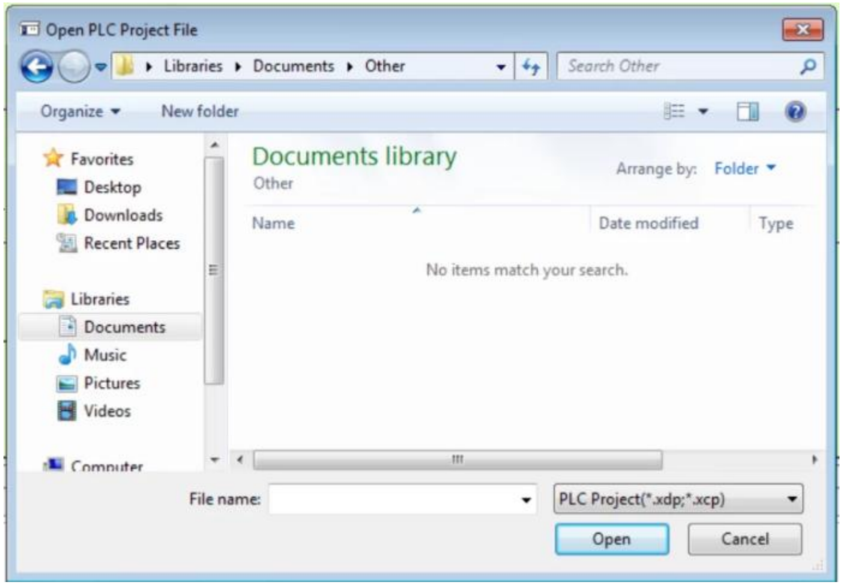
A XINJE PLC running in a lab setup.

Chaining Two Vulnerabilities to Load a Malicious File

Once we've constructed a suitable setup and finished researching the different protocols used by the equipment, we're often asked by our customers to look for security issues with the setup.

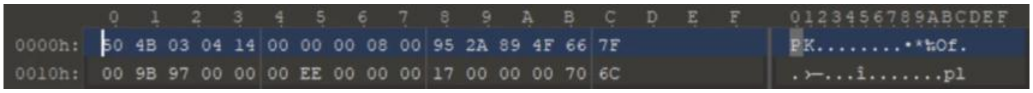
Pointing out these issues can help users improve their security posture immediately. Responsibly reporting these vulnerabilities to the vendor, can help fix them and improve security across the entire OT space.

In XINJE's case, we decided to focus on the engineering workstation program called XINJE PLC Program Tool. As mentioned earlier, in such cases project file vulnerabilities are of particular interest. Usually, searching for project file vulnerabilities begins with investigating the structure of the project file used by the engineering workstation program. In the case of XINJE PLC Program Tool, the relevant files are *.xdp files:



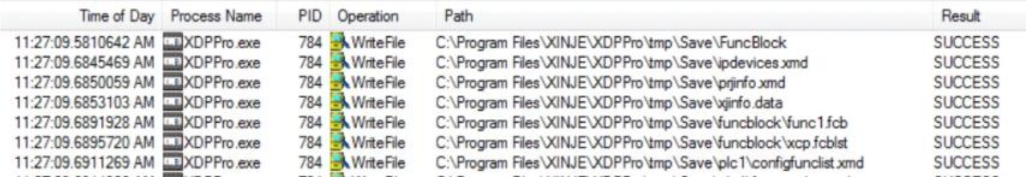
XINJE PLC project file structures are .xdp files.

These project files can be easily identified as zip files, as indicated by the PK\x03\x04 magic, below:



```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: 50 4B 03 04 14 00 00 00 08 00 95 2A 89 4F 66 7F   PK........•*‰Of.
0010h: 00 9B 97 00 00 00 EE 00 00 00 17 00 00 00 70 6C   .›—...î.......pl
```

And they can be extracted by almost any archive utility (e.g. 7z). What's even more interesting, is that when the the program opens a project file, it immediately extracts it to a temporary directory located within its installation directory:



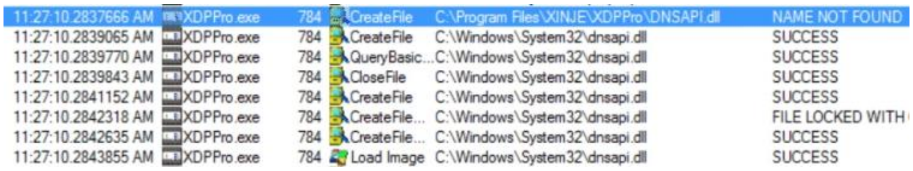
```
       Time of Day  Process Name   PID  Operation  Path                                                        Result
11:27:09.5810642 AM XDPPro.exe     784  WriteFile  C:\Program Files\XINJE\XDPPro\tmp\Save\FuncBlock             SUCCESS
11:27:09.6845469 AM XDPPro.exe     784  WriteFile  C:\Program 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 writes several files to C:\Program Files\XINJE\XDPPro\tmp

This behavior indicates that the program assumes it's being executed with administrator privileges. This, in combination with the extracted file being a zip file, immediately makes one wonder whether a zip slip vulnerability (an arbitrary file-overwrite vulnerability) can be leveraged to obtain arbitrary write privileges.

Soon enough we did find a zip slip vulnerability (**CVE-2021-34605**), which can provide an attacker with arbitrary write privileges with the permissions of the program; in most cases these will be administrator privileges.

The next question is how to reach code execution from an arbitrary file write. Since it makes the most sense for the code to be executed right after the project file is loaded, we can check what the program is doing while opening the project file:



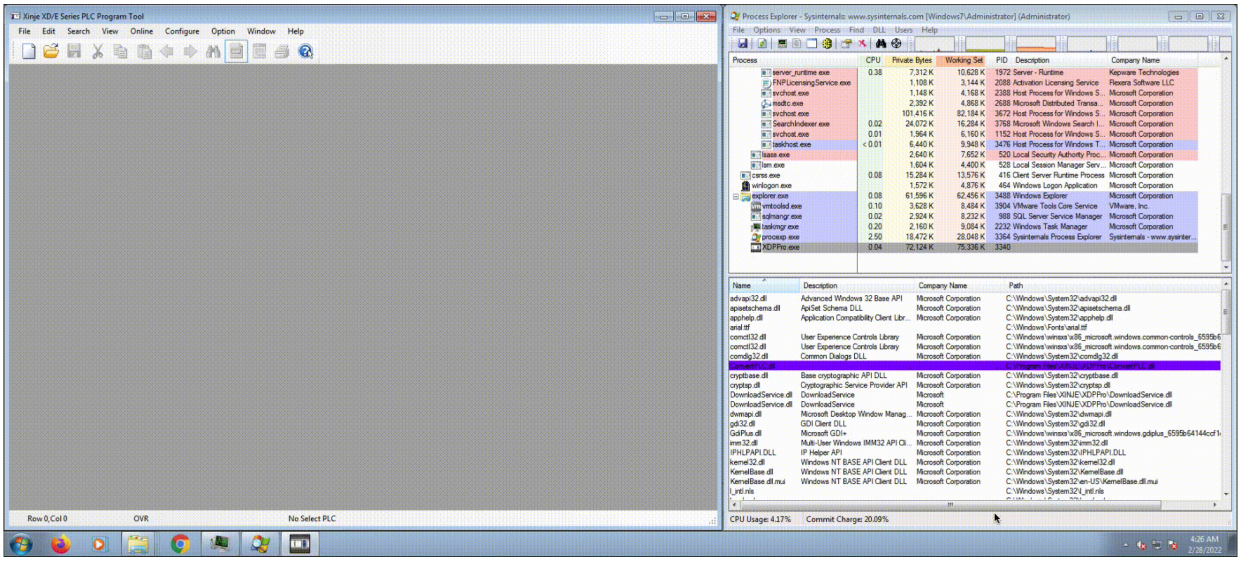
```
11:27:10.2837666 AM XDPPro.exe  784 CreateFile     C:\Program Files\XINJE\XDPPro\DNSAPI.dll  NAME NOT FOUND
11:27:10.2839065 AM XDPPro.exe  784 CreateFile     C:\Windows\System32\dnsapi.dll            SUCCESS
11:27:10.2839770 AM XDPPro.exe  784 QueryBasic...  C:\Windows\System32\dnsapi.dll            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 attempts to load DNSAPI.dll from C:\Program Files\XINJE\XDPPro, doesn't find it and falls back to C:\Windows\System32

Interestingly, it's trying to load .dll files from its local directory with LoadLibrary. When LoadLibrary doesn't find them, it reverts to searching for them in C:\Windows\System32. Here is where we found our second vulnerability, **CVE-2021-34606**, a classic DLL hijacking vulnerability.

In order to create a fully-working exploit, we chained our two vulnerabilities: Once a specially crafted malicious project file is opened by XINJE PLC Program Tool, the zip slip vulnerability will be triggered and a .dll file will be written to the program's directory in Program Files. Later in the process of loading a new project, this DLL will be loaded instead of the real DLL (located in Windows\System32).

Once the DLL is loaded, malicious code is executed during its DLLMain procedure or in one of the functions imported by the program. An attacker now may gain a foothold on an OT network.


Xinje XD/E Series PLC Program Tool
File Edit Search View Online Configure Option Window Help
Process Explorer - Sysinternals: www.sysinternals.com [Windows7\Administrator] (Administrator)
File Options View Process Find DLL Users Help
4:26 AM
2/28/2022

Row 0,Col 0 | OVR | No Select PLC

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
server_runtime.exe	0.38	7,312 K	10,628 K	1972	Server - Runtime	Kepware Technologies
FNPLicensingService.exe		1,108 K	3,144 K	2088	Activation Licensing Service	Flexera Software LLC
svchost.exe		1,148 K	4,168 K	2388	Host Process for Windows S...	Microsoft Corporation
msdtc.exe		2,392 K	4,868 K	2688	Microsoft Distributed Transa...	Microsoft Corporation
svchost.exe		101,416 K	82,184 K	3672	Host Process for Windows S...	Microsoft Corporation
SearchIndexer.exe	0.02	24,072 K	16,284 K	3768	Microsoft Windows Search I...	Microsoft Corporation
svchost.exe	0.01	1,964 K	6,160 K	1152	Host Process for Windows S...	Microsoft Corporation
taskhost.exe	< 0.01	6,440 K	9,948 K	3476	Host Process for Windows T...	Microsoft Corporation
lsass.exe		2,640 K	7,652 K	520	Local Security Authority Proc...	Microsoft Corporation
lsm.exe		1,604 K	4,400 K	528	Local Session Manager Serv...	Microsoft Corporation
csrss.exe	0.08	15,284 K	13,576 K	416	Client Server Runtime Process	Microsoft Corporation
winlogon.exe		1,572 K	4,876 K	464	Windows Logon Application	Microsoft Corporation
explorer.exe	0.08	61,596 K	62,456 K	3488	Windows Explorer	Microsoft Corporation
vmtoolsd.exe	0.10	3,628 K	8,484 K	3904	VMware Tools Core Service	VMware, Inc.
sqlmangr.exe	0.02	2,924 K	8,232 K	988	SQL Server Service Manager	Microsoft Corporation
taskmgr.exe	0.20	2,160 K	9,084 K	2232	Windows Task Manager	Microsoft Corporation
procexp.exe	2.50	18,472 K	28,048 K	3364	Sysinternals Process Explorer	Sysinternals - www.sysinter...
XDPPro.exe	0.04	72,124 K	75,336 K	3340		

Name	Description	Company Name	Path
advapi32.dll	Advanced Windows 32 Base API	Microsoft Corporation	C:\Windows\System32\advapi32.dll
apisetschema.dll	ApiSet Schema DLL	Microsoft Corporation	C:\Windows\System32\apisetschema.dll
apphelp.dll	Application Compatibility Client Libr...	Microsoft Corporation	C:\Windows\System32\apphelp.dll
arial.ttf			C:\Windows\Fonts\arial.ttf
comctl32.dll	User Experience Controls Library	Microsoft Corporation	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b6
comctl32.dll	User Experience Controls Library	Microsoft Corporation	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b6
comdlg32.dll	Common Dialogs DLL	Microsoft Corporation	C:\Windows\System32\comdlg32.dll
ConvertPLC.dll			C:\Program Files\XINJE\XDPPro\ConvertPLC.dll
cryptbase.dll	Base cryptographic API DLL	Microsoft Corporation	C:\Windows\System32\cryptbase.dll
cryptsp.dll	Cryptographic Service Provider API	Microsoft Corporation	C:\Windows\System32\cryptsp.dll
DownloadService.dll	DownloadService	Microsoft	C:\Program Files\XINJE\XDPPro\DownloadService.dll
DownloadService.dll	DownloadService	Microsoft	C:\Program Files\XINJE\XDPPro\DownloadService.dll
dwmapi.dll	Microsoft Desktop Window Manag...	Microsoft Corporation	C:\Windows\System32\dwmapi.dll
gdi32.dll	GDI Client DLL	Microsoft Corporation	C:\Windows\System32\gdi32.dll
GdiPlus.dll	Microsoft GDI+	Microsoft Corporation	C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1
imm32.dll	Multi-User Windows IMM32 API Cli...	Microsoft Corporation	C:\Windows\System32\imm32.dll
IPHLPAPI.DLL	IP Helper API	Microsoft Corporation	C:\Windows\System32\IPHLPAPI.DLL
kernel32.dll	Windows NT BASE API Client DLL	Microsoft Corporation	C:\Windows\System32\kernel32.dll
KernelBase.dll	Windows NT BASE API Client DLL	Microsoft Corporation	C:\Windows\System32\KernelBase.dll
KernelBase.dll.mui	Windows NT BASE API Client DLL	Microsoft Corporation	C:\Windows\System32\en-US\KernelBase.dll.mui
l_intl.nls			C:\Windows\System32\l_intl.nls

CPU Usage: 4.17% | Commit Charge: 20.09%

A demonstration of Team82's proof-of-concept exploit.

Wrapping Up

Despite the fact that awareness of cybersecurity has been steadily increasing in recent years in the OT world, many engineering workstation programs are still vulnerable to easily exploitable vulnerabilities.

Not all vendors are aware of the fact that project files can be weaponized by attackers as a method to take control of critical OT resources; this is true for most OT personnel as well.

In addition, many vendors still do not have well-defined interfaces for coordinated disclosure of vulnerabilities. As a result, disclosure can take an unnecessarily long time, often passing through sales and/or technical support teams without security knowledge, before reaching the teams responsible for the development of the affected products.

This was a challenging disclosure with XINJE, which thankfully is not the norm within the majority of OT vendors.

Share: □ □ □ □

Recent Vulnerability Disclosures

CVE-2022-40264

CVE-2022-3086

CVE-2022-38465

CVE-2022-41666

CVE-2022-41667

SOLUTIONS

Industrial Cybersecurity
Healthcare Cybersecurity
Commercial Cybersecurity

THREAT RESEARCH

Team82 Home
Vulnerability Disclosure Dashboard
Research
PGP Key

PARTNERS

Partners
Technology Alliance Partners
Channel Partners
Become a Partner
Find a Partner
Partner Login

RESOURCES

Resource Library
Blog
White Papers
Reports
Case Studies
Datasheets
Integration Briefs