

CVE-2022-35120

Incorrect Access Control in

IXPdata EasyInstall - 6.6.14725

Impact: can lead to local code execution or server compromise.

The software in question is a client management tool, utilizing a management server and clients connecting back to get updates, software and configurations. A vulnerability exists in the administrative tool, allowing for the decryption of secret login information.

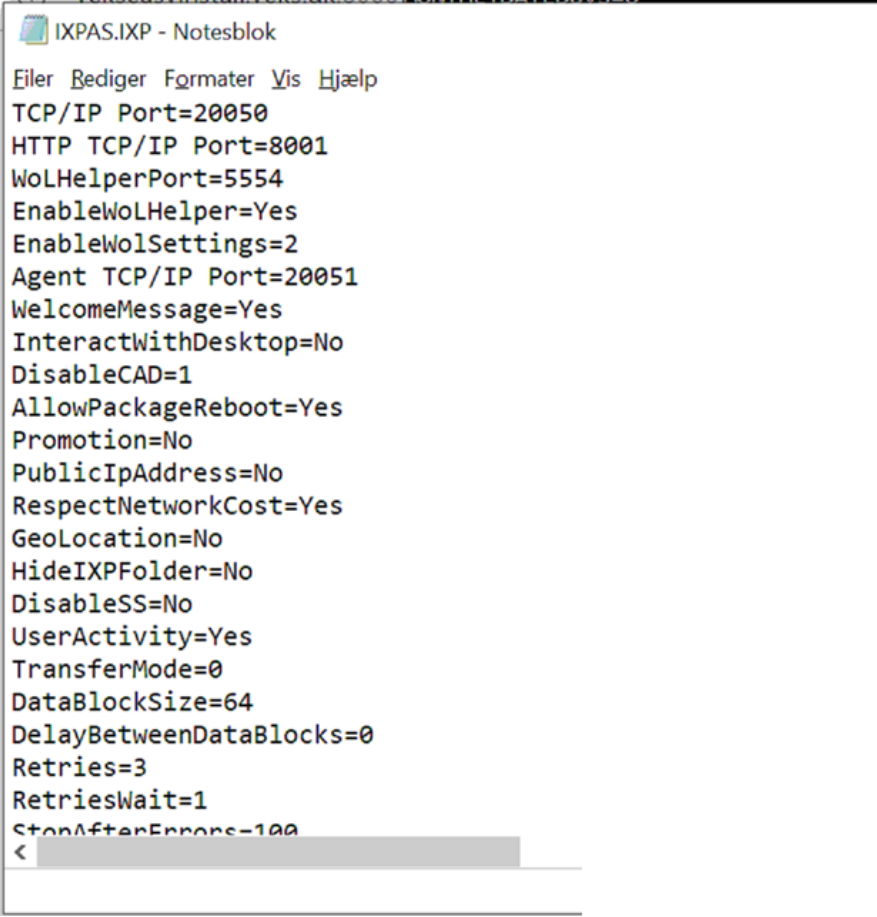
In order to obtain the tool inside a breached organisation, a chain of minor vulnerabilities is described below.

This version of the client software hides a configuration folder on the OS system drive but fails to set proper permissions on it, allowing an attacker to easily gather the information on how to browse the server once discovered.

The software can be set to block cmd.exe from launching but did not affect the ability to run Powershell ISE. Powershell can unhindered browse the filesystem and was unhindered in spawning cmd.exe as well.

A local configuration folder, c:\ixp\data, is hidden from the Windows Explorer, but fully visible in the command shells. The local user has permission to edit the files contained in the folder, and the variable HideIXPFolder in the client configuration can be set to No.

If an attacker changes the ports in use, the configuration will no longer be updated from the server and changed won't be overwritten.



```
IXPAS.IXP - Notesblok
Filer  Rediger  Formater  Vis  Hjælp
TCP/IP Port=20050
HTTP TCP/IP Port=8001
WoLHelperPort=5554
EnableWoLHelper=Yes
EnableWoLSettings=2
Agent TCP/IP Port=20051
WelcomeMessage=Yes
InteractWithDesktop=No
DisableCAD=1
AllowPackageReboot=Yes
Promotion=No
PublicIpAddress=No
RespectNetworkCost=Yes
GeoLocation=No
HideIXPFolder=No
DisableSS=No
UserActivity=Yes
TransferMode=0
DataBlockSize=64
DelayBetweenDataBlocks=0
Retries=3
RetriesWait=1
StopAfterErrors=100
<
```

This folder also contains the logs for communication with the server, revealing the direct IP for the (web)server hosting the server side of the product.

The main folder is hidden using a standard \$share, but the full path is visible in the logs. It's also in this case accessible directly from the webserver.

There is a lot of privileged information present here for an attacker to read:

## EasyInstall Directory of \

| Name   | Size      |
|--|-----------|
| <a href="#">Add to archive.lnk</a>               | 1,43 KB   |
| [AGENTS]   |           |
| [AUDIT]  |           |
| [AUTOMATION]                                     |           |
| [BACKUP]   |           |
| [BIN]  |           |
| [DOC]  |           |
| <a href="#">Extract here (in new folder).lnk</a> | 1,45 KB   |
| <a href="#">Extract here.lnk</a>                 | 1,42 KB   |
| <a href="#">Extract....lnk</a>                   | 1,45 KB   |
| [INVENTORY]                                      |           |
| [XPENROLL]                                       |           |
| <a href="#">XPES64.EXE.ori</a>                   | 19,8 MB   |
| [XPMENU]   |           |
| [LOGS]   |           |
| [NEW]  |           |
| <a href="#">Open as archive.lnk</a>              | 593 bytes |
| [PLUGINS]  |           |
| [PXF]  |           |

For example, the inventory folder leaks the hostnames of all connected machines.

| Navn | Ændringsdato     | Type     |
|------|------------------|----------|
| A    | 28-06-2022 13:40 | Filmappe |
| A    | 28-06-2022 13:13 | Filmappe |
| A    | 28-06-2022 00:20 | Filmappe |
| A    | 28-06-2022 09:31 | Filmappe |
| A    | 28-06-2022 14:56 | Filmappe |
| A    | 28-06-2022 10:27 | Filmappe |
| B    | 28-06-2022 15:03 | Filmappe |
| B    | 23-06-2022 12:00 | Filmappe |
| B    | 28-06-2022 07:39 | Filmappe |
| B    | 27-06-2022 14:54 | Filmappe |
| B    | 28-06-2022 14:13 | Filmappe |
| C    | 23-06-2022 14:07 | Filmappe |
| C    | 28-06-2022 15:21 | Filmappe |
| C    | 28-06-2022 14:17 | Filmappe |
| D    | 27-06-2022 10:56 | Filmappe |
| D    | 16-06-2022 04:17 | Filmappe |
| D    | 28-06-2022 12:37 | Filmappe |
| D    | 31-05-2022 08:53 | Filmappe |
| E    | 28-06-2022 15:13 | Filmappe |
| F    | 28-06-2022 14:08 | Filmappe |

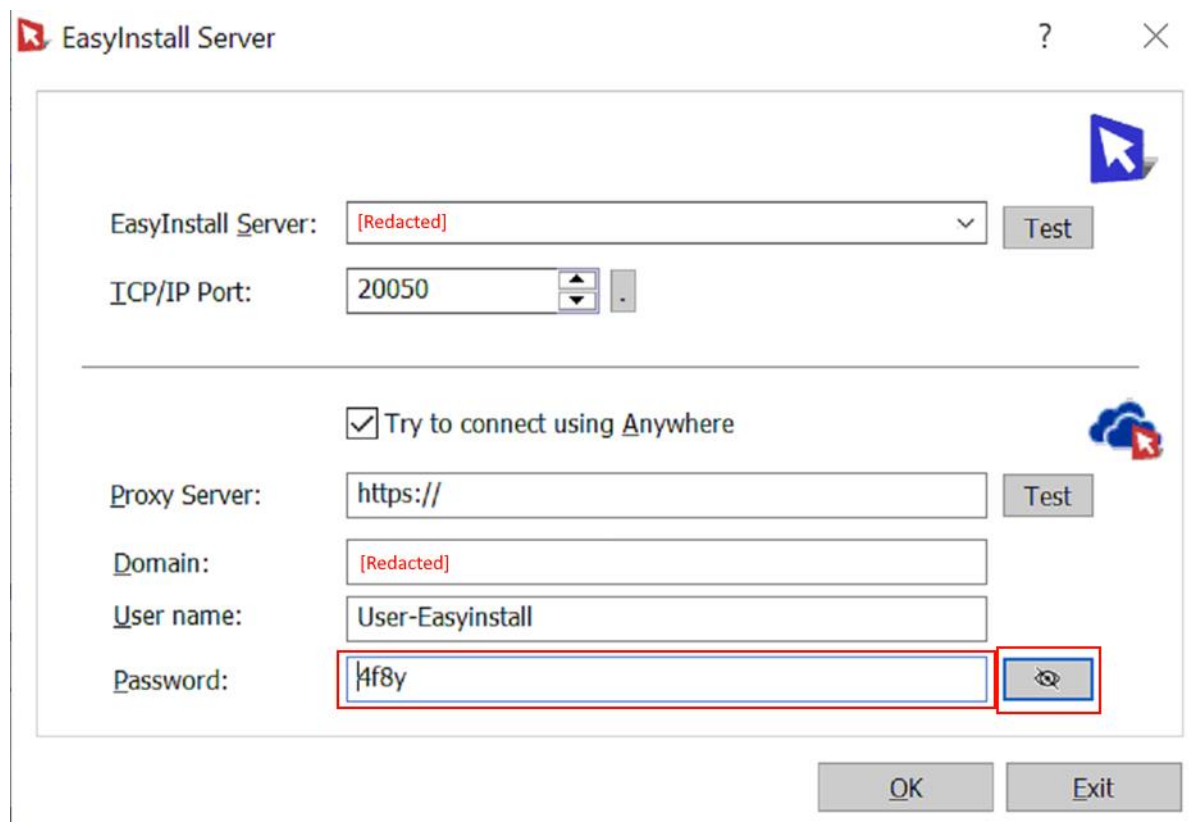
There is no hinderance for users in stealing the files from /BIN, and lets an attacker gather the administrative tools for the environment. This has unfortunate consequences.

### CVE-2022-35120

The “IXPADM64.exe” tool is a 16Mb “all-in-one” executable with a lot of functionality. A recent addition is the ability to generate strong passwords for the server and user-admin – and displaying cached information on the login prompt. This means that the executable must contain the key/certificates used to encrypt/decrypt this information.

On the client, sensitive information is cached in

HKLM\SOFTWARE\IXP\Agent\ClientID and can be viewed decrypted by clicking “Try to connect using Anywhere” and then the reveal password button.



This information is highly probable to be a local privilege escalation, lateral movement opportunity and possibly, if misconfigured, this may even lead to takeover of the server, which then leads to administrative rights on all clients.

In the environment where this was discovered, the User-EasyInstall was misconfigured to have too many privileges on the server, and it was then trivial to get obtain administrator access on the server.

**Fixes done by the software vendor – on the 1/7/2022:**

The local config file is no longer user-writable, and local sabotage is no longer possible.

The application now checks the account permissions, and alerts if misconfiguration is detected.

The username and password are no longer encrypted with the same key, so there is no easy way to decrypt the password.