

Windows

CVE

3 (

CVE)

/

**"C:\Program Files" C:\Program Files Windows C:\Program "C:\Program Files\Weak Services\Unquoted Service.exe"**

**C:\Program.exe**

**C:\Program Files\Weak.exe**

**C:\Program Files\Weak Services\Unquoted.exe**

**"C:\A B\C D\E F.exe"**

**C:\ A.exe C:\A.exe**

**C:\A" B" C.exe "C:\A B\C.exe"**

**"C:\A B\C D\" E.exe C:\A B\C D\E.exe"**

CVE CVE-2022-37197 <https://www.exploit-db.com/exploits/51029>) **C:\Program Files (x86)\IOTransfer\Updater\IOTUpdater.exe**

```
C:\>wmic service get name,displayname,pathname,startmode | findstr /i "auto" | findstr /i /v  
"c:\windows\\" | findstr /i /v ""
```

```
IOTransfer Updater IOTUpdaterSvc C:\Program Files (x86)\IOTransfer\Updater\IOTUpdater.exe  
Auto
```

```
C:\>sc qc IOTUpdaterSvc  
[SC] QueryServiceConfig SUCCESS
```

```
SERVICE_NAME: IOTUpdaterSvc  
        TYPE : 10 WIN32_OWN_PROCESS  
        START_TYPE : 2 AUTO_START  
        ERROR_CONTROL : 1 NORMAL  
        BINARY_PATH_NAME : C:\Program Files (x86)\IOTransfer\Updater\IOTUpdater.exe
```

```
LOAD_ORDER_GROUP :  
        TAG : 0  
        DISPLAY_NAME : IOTransfer Updater  
        DEPENDENCIES :  
        SERVICE_START_NAME : LocalSystem
```

**CVE-2021-35312** <https://www.exploit-db.com/exploits/50184>):

## Amica Prodigy 1.7 - Privilege Escalation

**EDB-ID:**

50184

**CVE:**

2021-35312

**Author:**

ANDREA INTILANGELO

**Type:**

LOCAL

**Platform:**

WINDOWS

**Date:**

2021-08-10

**EDB Verified:** ✕**Exploit:** 📄 / {}**Vulnerable App:**

```
# Exploit Title: Amica Prodigy 1.7 - Privilege Escalation
# Date: 2021-08-06
# Exploit Author: Andrea Intilangelo
# Vendor Homepage: https://gestionaleamica.com - https://www.bisanziosoftware.com
# Software Link: https://gestionaleamica.com/Download/AmicaProdigySetup.exe
# Version: 1.7
# Tested on: Windows 10 Pro 20H2 x64
# CVE: CVE-2021-35312
```

Amica Prodigy it's a backup solution from Amica softwares (GestionaleAmica: invoices, accounting, etc., from website [gestionaleamica.com](https://gestionaleamica.com)), a CIR 2000 srl / Bisanzio Software srl

A vulnerability was found in CIR 2000 / Gestionale Amica Prodigy v1.7. The Amica Prodigy's executable "RemoteBackup.Service.exe" has incorrect permissions, allowing a local unprivileged user to replace it with a malicious file that will be executed with "LocalSystem" privileges at scheduled time.

```
C:\Users\user>icacls C:\AmicaProdigy\RemoteBackup.Service.exe
```

```
C:\AmicaProdigy\RemoteBackup.Service.exe
NT AUTHORITY\Authenticated Users:(I)(M) NT
AUTHORITY\SYSTEM:(I)(F) BUILTIN\Administrators:(I)(F)
BUILTIN\Users:(I)(RX) Elaborazione completata per 1 file.
```

### RemoteBackup.Service.exe

### SYSTEM

### powerup.ps1

Revision #4

Created 5 September 2022 03:02:05 by

Updated 14 March 2023 17:15:48 by