

ZKTeco ZKTime.Net 3.0.1.6 Insecure File Permissions

2016.08.31		
Credit: Gjoko 'LiquidWorm' Krstic (https://cxsecurity.com/author/Gjoko+%26%23039%3BLiquidWorm%26%23039%3B+Krstic/1/)		
Risk: <input type="text" value="Low"/>	Local: <input type="text" value="Yes"/>	Remote: <input type="text" value="No"/>
CVE: <input type="text" value="N/A"/>	CWE: <input type="text" value="N/A"/>	

ZKTeco ZKTime.Net 3.0.1.6 Insecure File Permissions

Vendor: ZKTeco Inc. | Xiamen ZKTeco Biometric Identification Technology Co.,ltd

Product web page: <http://www.zkteco.com>

Affected version: 3.0.1.6

3.0.1.5 (160622)

3.0.1.1 (160216)

Summary: ZKTime.Net V3.0 is a new generation time attendance management software. Meanwhile, it integrates with time attendance and access control system. Some frequently used functions such as attendance reports, device management and employee management can be managed directly on the home page which providing excellent user experience. Owing to the Pay code function, it can generate both time attendance records and corresponding payroll in the software and easy to merge with the most ERP and Payroll software, which can rapidly upgrade your working efficiency. The brand new flat GUI design and humanized structure will make your daily management more pleasant and convenient.

Desc: ZKTime.Net suffers from an elevation of privileges vulnerability

y
which can be used by a simple user that can change the executable file
with a binary of choice. The vulnerability exist due to the improper
permissions, with the 'C' flag (Change) for 'Everyone' group, making the
entire directory 'ZKTimeNet3.0' and its files and sub-dirs world-writable.

**Tested on: Microsoft Windows 7 Ultimate SP1 (EN)
Microsoft Windows 7 Professional SP1 (EN)**

**Vulnerability discovered by Gjoko 'LiquidWorm' Krstic
@zeroscience**

Advisory ID: ZSL-2016-5360

Advisory URL: <http://www.zeroscience.mk/en/vulnerabilities/ZSL-2016-5360.php>

18.07.2016

--

```
C:>showacls "c:Program Files (x86)ZKTimeNet3.0"
c:Program Files (x86)ZKTimeNet3.0
          Everyone                Change [RWXD]
          NT SERVICETrustedInstaller Special Access [A]
          NT AUTHORITYSYSTEM       Special Access [A]
          BUILTINAdministrators    Special Access [A]
          BUILTINUsers             Special Access [RX]
          CREATOR OWNER            Special Access [A]
```

```
C:>showacls "c:Program Files (x86)ZKTimeNet3.0ZKTimeNet.exe"
c:Program Files (x86)ZKTimeNet3.0ZKTimeNet.exe
          Everyone                Change [RWXD]
```

```

C:\Program Files (x86)>cacls ZKTimeNet3.0
C:\Program Files (x86)\ZKTimeNet3.0 Everyone:(OI)(CI)C
                                NT SERVICE\TrustedInstaller:(ID)F
                                NT SERVICE\TrustedInstaller:(CI)(I
0)(ID)F
                                NT AUTHORITY\SYSTEM:(ID)F
                                NT AUTHORITY\SYSTEM:(OI)(CI)(IO)(I
D)F
                                BUILTIN\Administrators:(ID)F
                                BUILTIN\Administrators:(OI)(CI)(I
0)(ID)F
                                BUILTIN\Users:(ID)R
                                BUILTIN\Users:(OI)(CI)(IO)(ID)(spe
cial access:)
                                                                GEN
ERIC_READ
                                                                GEN
ERIC_EXECUTE
                                CREATOR OWNER:(OI)(CI)(IO)(ID)F

```

```

C:\Program Files (x86)\ZKTimeNet3.0>cacls *.exe
C:\Program Files (x86)\ZKTimeNet3.0\LanguageTranslate.exe Everyone:C
                                                                Everyone:(I
D)C
                                                                NT AUTHORITY\
SYSTEM:(ID)F
                                                                BUILTIN\Admi
nistrators:(ID)F
                                                                BUILTIN\User
s:(ID)R
C:\Program Files (x86)\ZKTimeNet3.0\unins000.exe Everyone:(ID)C
                                                                NT AUTHORITY\SYSTEM:
(ID)F
                                                                BUILTIN\Administrator

```

s: (ID)F

BUILTINUsers: (ID)R

C:Program Files (x86)ZKTimeNet3.0ZKTimeNet.DBTT.exe Everyone:C

Everyone: (ID)C

NT AUTHORITYSY

STEM: (ID)F

BUILTINAdminis

trators: (ID)F

BUILTINUsers:

(ID)R

C:Program Files (x86)ZKTimeNet3.0ZKTimeNet.exe Everyone:C

Everyone: (ID)C

NT AUTHORITYSYSTEM:

(ID)F

BUILTINAdministrato

rs: (ID)F

BUILTINUsers: (ID)R

C:Program Files (x86)ZKTimeNet3.0ZKTimeNet.Update.exe Everyone:C

Everyone: (I

D)C

NT AUTHORITY

SYSTEM: (ID)F

BUILTINAdmin

istrators: (ID)F

BUILTINUser

s: (ID)R

C:Program Files (x86)ZKTimeNet3.0ZKTimeNet.ZKTime5DB.exe Everyone:C

Everyone:

(ID)C

NT AUTHOR

ITYSYSTEM: (ID)F

BUILTINAd

ministrators: (ID)F

BUILTINUs

ers: (ID)R

See this note in RAW Version (<https://cxsecurity.com/ascii/WLB-2016080264>)

Vote for this issue:

50%

50%

Comment it here.

Nick (*)

Email (*)

Video

Text (*)