

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

ZKTeco ZKTime.Net 3.0.1.6 - Insecure File Permissions Privilege Escalation

EDB-ID:

40322

CVE:

N/A

EDB Verified: ✘

Author:

[LIQUIDWORM](#)

Type:

[LOCAL](#)

Exploit:  

Platform:

[WINDOWS](#)

Date:

2016-08-31

Vulnerable App:



 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

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 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 SERVICE\TrustedInstaller Special Access [A]
NT AUTHORITY\SYSTEM     Special Access [A]
BUILTIN\Administrators  Special Access [A]
BUILTIN\Users           Special Access [RX]
CREATOR OWNER           Special Access [A]
```

```
C:\>showacls "c:\Program Files (x86)\ZKTimeNet3.0\ZKTimeNet.exe"
c:\Program Files (x86)\ZKTimeNet3.0\ZKTimeNet.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)(IO)
(ID)F
```



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```

NT AUTHORITY\SYSTEM:(ID)F
NT AUTHORITY\SYSTEM:(OI)(CI)(IO)(ID)F
BUILTIN\Administrators:(ID)F
BUILTIN\Administrators:(OI)(CI)(IO)

(ID)F

BUILTIN\Users:(ID)R
BUILTIN\Users:(OI)(CI)(IO)(ID)(special
access:))

GENERIC_READ

GENERIC_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:(ID)C
NT
AUTHORITY\SYSTEM:(ID)F
BUILTIN\Administrators:(ID)F
BUILTIN\Users:
(ID)R
C:\Program Files (x86)\ZKTimeNet3.0\unins000.exe Everyone:(ID)C
NT AUTHORITY\SYSTEM:(ID)F
BUILTIN\Administrators:
(ID)F
BUILTIN\Users:(ID)R
C:\Program Files (x86)\ZKTimeNet3.0\ZKTimeNet.DBTT.exe Everyone:C
Everyone:(ID)C
NT AUTHORITY\SYSTEM:
(ID)F
BUILTIN\Administrators:(ID)F
BUILTIN\Users:(ID)R
C:\Program Files (x86)\ZKTimeNet3.0\ZKTimeNet.exe Everyone:C
Everyone:(ID)C
NT AUTHORITY\SYSTEM:(ID)F
BUILTIN\Administrators:
(ID)F
BUILTIN\Users:(ID)R
C:\Program Files (x86)\ZKTimeNet3.0\ZKTimeNet.Update.exe Everyone:C
Everyone:(ID)C
NT
AUTHORITY\SYSTEM:(ID)F
BUILTIN\Administrators:(ID)F
BUILTIN\Users:
(ID)R
C:\Program Files (x86)\ZKTimeNet3.0\ZKTimeNet.ZKTime5DB.exe Everyone:C
Everyone:(ID)C
NT
AUTHORITY\SYSTEM:(ID)F
BUILTIN\Administrators:(ID)F
BUILTIN\Users:
(ID)R

```

Tags:

Advisory/Source: [Link](#)

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING



Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

[COOKIES](#) ©

[OffSec Services Limited](#) 2026. All rights reserved.