

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

ZKTeco ZKAccess Professional 3.5.3 - Insecure File Permissions Privilege Escalation

EDB-ID:

40323

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

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

ZKTeco ZKAccess Professional 3.5.3 Insecure File Permissions

Vendor: ZKTeco Inc. | Xiamen ZKTeco Biometric Identification Technology Co.,ltd
 Product web page: <http://www.zkteco.com>
 Affected version: 3.5.3 (Build 0005)

Summary: ZKAccess 3.5 is a desktop software which is suitable for small and medium businesses application. Compatible with all ZKAccess standalone reader controllers, the software can simultaneously manage access control and generate attendance report. The brand new flat GUI design and humanized structure of new ZKAccess 3.5 will make your daily management more pleasant and convenient.

Desc: ZKAccess suffers from an elevation of privileges vulnerability which can be used by a simple authenticated user that can change the executable file with a binary of choice. The vulnerability exist due to the improper permissions, with the 'M' flag (Modify) for 'Authenticated Users' group.

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

Vulnerability discovered by Gjoko 'LiquidWorm' Krstic
 @zeroscience

Advisory ID: ZSL-2016-5361
 Advisory URL: <http://www.zeroscience.mk/en/vulnerabilities/ZSL-2016-5361.php>

18.07.2016

--

```
C:\ZKTeco>icacls ZKAccess3.5
ZKAccess3.5 BUILTIN\Administrators:(I)(F)
             BUILTIN\Administrators:(I)(OI)(CI)(IO)(F)
             NT AUTHORITY\SYSTEM:(I)(F)
             NT AUTHORITY\SYSTEM:(I)(OI)(CI)(IO)(F)
             BUILTIN\Users:(I)(OI)(CI)(RX)
             NT AUTHORITY\Authenticated Users:(I)(M)
             NT AUTHORITY\Authenticated Users:(I)(OI)(CI)(IO)(M)
```

Successfully processed 1 files; Failed processing 0 files

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.