

## iDS6 DSSPro Digital Signage System 6.2 Password Disclosure

2020.11.05		
🚩 <a href="https://cxsecurity.com/author/LiquidWorm/1/">LiquidWorm (https://cxsecurity.com/author/LiquidWorm/1/)</a> (MK) 🚩		
Risk: <input type="text" value="High"/>	Local: <input type="text" value="No"/>	Remote: <input type="text" value="Yes"/>
<u>CVE</u> : N/A	<u>CWE</u> : N/A	

### iDS6 DSSPro Digital Signage System 6.2 (autoSave) Cookie User Password Disclosure

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 cleartext transmission/storage of

sensitive information in a cookie when using the Remember (autoSave=true)

feature. This allows a remote attacker to intercept the HTTP Cookie

authentication credentials via a man-in-the-middle attack.

**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-2020-5605

Advisory URL: <https://www.zeroscience.mk/en/vulnerabilities/ZSL-2020-5605.php>

16.07.2020

--

For regular dashboard (Cookie: cookie.username, cookie.password):  
-----

```
GET /Pages/user.action HTTP/1.1
Host: 192.168.1.88
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.1.1/Pages/playlog.action
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,mk;q=0.8
```

Cookie: cookie.cstm=demo; cookie.username=joxy; cookie.password=12312123; cookie.autosave=true; cookie.autologin=true; JSESSIONID=63306896AC4A2E193231297D60813C8D

For admin dashboard (Cookie: cookie.admin.username, cookie.admin.password):

-----  
-----

POST /admin/customer!list HTTP/1.1  
Host: 192.168.1.88  
Connection: keep-alive  
Content-Length: 56  
Accept: application/json, text/javascript, \*/\*; q=0.01  
X-Requested-With: XMLHttpRequest  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.111 Safari/537.36  
Content-Type: application/x-www-form-urlencoded; charset=UTF-8  
Origin: http://192.168.1.88  
Referer: http://192.168.1.88/admin/customer.action  
Accept-Encoding: gzip, deflate  
Accept-Language: en-US,en;q=0.9,mk;q=0.8  
Cookie: cookie.admin.username=admin; cookie.admin.password=123456; cookie.admin.autosave=true; JSESSIONID=604A85C99BF10F385D74FECF501F5E05

**See this note in RAW Version** (<https://cxsecurity.com/ascii/WLB-2020110023>)

Post

Vote for this issue:

 0	 0
50%	50%

## Comment it here.

---

**Nick (\*)**

**Email (\*)**

**Video**

**Text (\*)**

---

Copyright 2026, cxsecurity.com