

QiHang Media Web Digital Signage 3.0.9 Password Disclosure

2020.08.14		
🚩 LiquidWorm (https://cxsecurity.com/author/LiquidWorm/1/) (MK) 🚩		
Risk: <input type="text" value="Medium"/>	Local: <input type="text" value="No"/>	Remote: <input type="text" value="Yes"/>
<u>CVE</u> : N/A	<u>CWE</u> : N/A	

QiHang Media Web (QH.aspx) Digital Signage 3.0.9 Cookie User Password Disclosure

Vendor: Shenzhen Xingmeng Qihang Media Co., Ltd.

Guangzhou Hefeng Automation Technology Co., Ltd.

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

Affected version: 3.0.9.0

Summary: Digital Signage Software.

Desc: The application suffers from a cleartext transmission/storage of sensitive information in a cookie. This allows a remote attacker to intercept the HTTP Cookie authentication credentials via a man-in-the-middle attack.

Tested on: Microsoft Windows Server 2012 R2 Datacenter

Microsoft Windows Server 2003 Enterprise Edition

ASP.NET 4.0.30319

HowFor Web Server/5.6.0.0

Microsoft ASP.NET Web QiHang IIS Server

**Vulnerability discovered by Gjoko 'LiquidWorm' Krstic
@zeroscience**

Advisory ID: ZSL-2020-5578

Advisory URL: <https://www.zeroscience.mk/en/vulnerabilities/ZSL-2020-5578.php>

27.07.2020

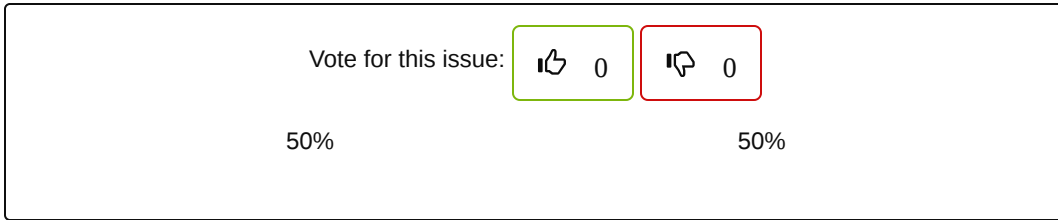
--

Intercepted request:

POST /QH.aspx HTTP/1.1
Host: 192.168.1.74:8090
Content-Length: 127
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.89 Safari/537.36
X-Requested-With: XMLHttpRequest
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept: */*
Origin: http://192.168.1.74:8090
Referer: http://192.168.1.74:8090/index.htm
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: ASP.NET_SessionId=3c15wuu2incsgmfmzr0ziff; qihang_cookie_key_account=admin; qihang_cookie_key_password=admin; qihang_cookie_key_language=en; qihang_cookie_key_auto_login=
Connection: close

[See this note in RAW Version](https://cxsecurity.com/ascii/WLB-2020080059) (<https://cxsecurity.com/ascii/WLB-2020080059>)

Post



Comment it here.

Nick (*)

Email (*)

Video

Text (*)