IEGEEK SECURITY VULNERABILITIES STILL PREVALENT IN 2022 IG20

6 Comments / Data Security, Featured, How to, InfoSec News, Vulnerabilities / By RiSec.n0tst3

Table of Contents

Amazon's "highly rated", "recommended" ieGeek brand continues to present a number of security vulnerabilities.

ieGeek Security Vulnerabilities

On the 19th of Aug 2022 I set out to purchase a CCTV Camera from Amazon, I read over the reviews of the ieGeek IG20, and it seemed great, the value too. For just £29.99 I'd get myself a great looking CCTV Camera, packed full of features. It has night vision, Smartphone access, Motion Detection, Plug & Play, It's waterproof and it can connect via WiFi or Ethernet. Great, I was sold. However, I failed to do any research on the brand specifically.

The camera arrived the following day, and later that day I got around to setting it up. I first noticed that on the back of the camera, there was a sticker with a UID printed, along with a Factory default Username & Password combination, consisting of admin/admin.

ieGeek IG20 Issues/Vulnerabilities

UID Weakness CWE-340 – CVE-2022-38970

The UID appears to be predictable. The UID in our case will look like this: `AAFF-123456-ABCDE` – depending on the make and model.

- UID p1: *Same 4 letters at the start.*
- UID p2: *6 numbers at random in the middle.*
- UID p3: *5 random letters at the end.*

Evidently, having just this basic knowledge of the UID and using the default credentials, the camera feed could be accessed using the software provided by ieGeek from their website by testing each UID

Below are some more vulnerable prefixes running the same crappy firmware.

AAAA	AABB	AACC	AAES	AIPC
AAFF	BBBB	CAM	CAMERA	CCCC
DDDD	DEAA	EEEE	ELSA	ELSO
ESCM	ESN	ESS	EUA	EYE
FCARE	FDTAA	FFFF	FOUS	GCAM
GCMN	GGGG	GKW	HHHH	HRXJ
HSL	HVC	HWAA	HZD	HZDA
HZDB	HZDC	HZDN	HZDX	HZDY
HZDZ	IIII	ISRP	JWEV	MCI
MDI	MFIA	MMMM	MSF	MSI

SSAA	SSSS	SURE	SXH	TTTT
UUUU	VIEW	VSTA	VSTB	VSTC
VSTD	VSTF	WCAM	WGKJ	WHI
WNR	WNS	WNV	WWWW	WXH
WXO	XCPTP	XHA	XLT	XWL
ZLD	ZZZZ	AVA		

Unauthenticated / Default auth access to camera stream via RTSP protocol CWE-284

By default, one can easily access the camera's stream externally or internally depending on your router/network configuration, with our without means of Authentication.

- **Zero Authentication:** rtsp://+IP+/11
- **Default Auth:** rtsp://admin:admin@+IP+/11

Replace +IP+ with your local or external IP.

Here is a screenshot of the Default RTSP settings, requiring Zero authentication.

The cloud function of the camera uses the P2P protocol to send and make requests back to a server based in China in plaintext. It was found that all connections back to this were made in plaintext regardless of protocol, this includes the viewing of the camera's stream and control. HTTPS was not found to be implemented anywhere on the camera.

Access to files stored on the camera CWE-284

The following directories can be viewed using the default login:

- http://+IP+/tmpfs
- http://+IP+/js
- http://+IP+/lib
- http://+IP+/log
- http://+IP+/resources
- http://+IP+/sd
- http://+IP+/swfs

The number of links discovered showed that the SD card, log files and website front-end code were accessible from the web interface. This includes any footage that has been recorded by the device and stored on the external SD card.

possible for each of these devices to be accessed via default credentials, or if the admin credentials are changed, Using VLC player, I could potentially connect to each of these camera streams without the need to authenticate.

Admin Panel – Basic Authentication in use / Weak Password Requirements CWE-521 / CWE-287

When the camera is booted up, a web server is spawned and requires a login to gain access. Default credentials were then used to gain access and there was no setup to force change of the default password in place. Burpsuite caught this login process; the session was found to be using HTTP Basic Authentication to handle the username and password. The Base64 translates to admin:admin.

JavaScript injection (DOM-based) CWE-79

Data is read from **document.cookie** and passed to **eval()**

```
var strCookie=document.cookie;
var arrCookie=strCookie.split('; ');
var arr=arrCookie[i].split('=');
return unescape(arr[1]);
var cooktype=getcookie('cookmun');
var string = eval("'cgi-bin/hi3510/param.cgi?cmd=setimageattr&-
image_type="+cooktype+"&-default=on'");
```

Using various different methods of escaping. Stored XSS was also prevalent in many places within the admin panel that used user input. Example: FTP Upload settings.

HTTP Response Header Injection/Splitting CWE-644

The web application is also evidently vulnerable to HTTP response header injection, see PoC below. This also led me to discover i was able to break out of the response.

Your options for exploitation vary depending on the type of response you're injected into and also

Here we've added a "malicious cookie" which will be set in the browser. As mentioned earlier i was also able to break into the body, or out of the headers through double CRLFs (%0d%0a%0d%0a) ***see below***.

When user input is insecurely inserted into the headers of server responses, HTTP Header Injection vulnerabilities are created. They are based on the theory that an attacker can make the server generate a response that contains carriage-return and line-feed characters (or, respectively, %0D and %0A in their URI encoded forms), within the server response header, and/or that the attacker may be able to add specially created headers. Attacks like response splitting, session fixation, cross-site scripting, and malicious redirection are all possible using header injection.

Often, the injection of headers is not the main attack; rather, it is merely a method for accessing or exploiting another flaw. For instance, if a hacker is able to inject a payload through HTTP header

```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-08-28 00:42 BST
Nmap scan report for 192.168.1.116
Host is up (0.0088s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
80/tcp   open  http Hipcam RealServer/V1.0
554/tcp  open  rtsp
1935/tcp open  rtmp Real-Time Messaging Protocol
8080/tcp open  http-proxy ONVIFservice
MAC X (Shenzhentong BO Weitechnology) SHENZHEN TONG BO WEI
TECHNOLOGY Co.,LTD
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10
Network Distance: 1 hop
```

Anyway, I decided enough is enough with this trash device and unplugged it from my network, packaged it back up and arranged a return with Amazon.

The Listing On Amazon

At the time of writing, the listing is still available, however, I reached out to Amazon and made them fully aware of everything, including my intention to publish this article, and they advised me that the product listing would be "temporarily" removed today, 28th Aug 2022, pending further Investigation. The listing can be seen here *[if still available]*

It has to be worth noting, that there was an investigation by Which.co.uk see reference [3] in July 2021, that details a line of similar flaws, consequently, Amazon removed the said ieGeek branded camera from sale on its website. The which? investigation revealed another device from the same manufacturer can be easily hacked by cybercriminals.

> *The £40 camera, which was labelled Amazon's Choice, had more than 8,500 reviews (as of June 22 2021), including 68% giving the full five stars.*
>
> *If you own the ieGeek Security Outdoor Camera 1080p, you should change its default password immediately, or better still, stop using it.*
>
> *https://www.which.co.uk/news/article/iegeek-security-camera-removed-from-sale-following-which-investigation-ajW4t0g7bnGj*

So the question remains, why do Amazon allow Manufacturers to list products irrelevant of the manufacturer having been Flagged, and Delisted in the past? A better system needs to be in place. Yes, I understand there can be a new line of products/models but surely amazon should be seen to be doing more to prevent devices like this from appearing on their website. The privacy and security of their customers should be paramount.

Recommended: Global Mobile Network Vulnerabilities Affect All Cellular Generations Since 2G

Update 01 Sep 2022 – Product Still

Here is the screenshot of a mail I received from the Amazon Representative on the 28th of August, this email states the item “may be temporarily unavailable”, which contradicts what she told me on the telephone. This email arrived in my mailbox very shortly after I had a call with the same lady, Roxy.

Update: 01 Sep 2022

We’ve been made aware of another article from Which.co.uk, this second article was published in late 2021, after the earlier-mentioned article. Their second write-up clearly paints a very different picture, one could easily say it’s misleading given what has been uncovered in this report. It has to be worth mentioning that my ieGeek device, and probably many many others, was still running the same vulnerability-ridden firmware that Which.co.uk spoke out against in their first write-up, as has been verified by the team here at risec and elsewhere. There was no obvious offer of any firmware upgrade, at least to my knowledge. Anyway, see some quotes from the second write-up below.

> *HiChip has agreed to enforce a strong password policy, particularly blocking generic terms such as 'password' and 'admin'.*
>
> *For CamHi devices that are already set up in people's homes, the app will remind them to change the default password and warn them if what they have chosen is weak*
>
> ***MISLEADING**: https://www.which.co.uk/news/article/millions-of-camhi-wireless-cameras-made-more-secure-after-hacking-risk-aezzW2u2ELsl*

We have reached out to Which.co.uk and have yet to receive any notable response.

Consumer Recommendations

If you value your privacy, and security as much as we do, please remove the device from service. It is simply unfit for purpose. If you bought it from Amazon, go and arrange a return as this device is in clear breach of their merchant conditions.

Research each device thoroughly before buying, and check it's security reputation.

***Be Aware:** Endless numbers of IP cameras of other Brands also use the Hipcam RealServer service; I am unable to check the configuration of these devices specifically, but one would be led to believe they are all implemented similarly. Sadly, there doesn't seem to be a method to warn anyone utilising these IP Cameras that they are exposed.*

On a final note, take amazon's reviews with a pinch of salt, and always do your homework. Next time your about to purchase a connected device, IoT(Internet-of-Things), do a quick google query, something like, "vulnerable BRAND" or "exploit BRAND"

Q&A

they lack proper encryption, and, are shipped to consumers riddled with security holes. One can only ask themselves, is it intentional? *tldr; Given the research of the team here at RiSec, and research conducted elsewhere, we can categorically say ieGeek's cameras are not secure in 2022.*

What are the real risks of ieGeek cameras?

By using these devices that lack proper safety and security standards, your private data is at serious risk of being exposed, **a bad actor may able to gain complete control of the cameras**. This fundamentally opens up your entire network to further attack, making it much easier for a bad actor to reach an end goal.

Recommended: Safari 15 Vulnerability Allows Cross-Site Tracking of Users

Cheap CCTV cameras tend to be vulnerable to at least one of the following types of hacking:

1. They have a weak default password and username setting, which can be easily discoverable. If the user doesn't change those settings, it's very easy for hackers to find their way into your camera control system, in every case, there is no prompt in the Admin panel when logging in, advising you to chase any password.
2. They don't encrypt your data so that your home router password input is un-encrypted and accessible to any cyber attacker, or themselves.., same applies with any SMTP email info provided, along with any FTP info provided to the device. By using the home router password, they can gain access to other devices on your home network, can monitor your Internet history and any stored data on connected devices.
3. They let external users gain root access to the device itself, allowing hackers to take control,

Cheap CCTV Invites Outside Threats Into Your Home[4]

> *There are three main security issues you need to look for when buying your CCTV camera. Popular wireless security camera brands that are sold on online marketplaces like Amazon, but also eBay share common security flaws.*
>
> *As a rule of thumb, brands that are not well-known outside of the online market should be avoided at all cost. Affordable CCTV solutions from Shenzhen-based factories in China sometimes fail to meet wireless safety standards.*
>
> *Brands that have been tested for vulnerability and that you should avoid are the following; ieGeek, Sricam, SV3C, and Vstarcam. All come with a friendly price tag, but they are quick to join the list of CCTV cameras that put your privacy and security at risk.*
>
> *Tested by a professional security lab, Context Information Security, "cheap CCTV cameras show that they fail to prioritise customers' security even those that are bestsellers in online marketplaces"*
>
> *[4]*

Update: ***21/09/2022*** – After some back-and-forth correspondence with the vendor, ***ieGeek***, they have disputed that the ieGeek IG20 is an insecure device, despite our evidence to the contrary, they also cited an invalid misleading Which.co.uk[5] post as seen above.

Coming up next, I will be covering a Chinese "Mini-PC" that was shipped to me loaded with Malware.

Ciao, for now.

References

Amazon product listing[1]

IG20 ieGeek store page[2]

Which investigation ieGeek[3]

Cheap CCTV Sold With Known Vulnerabilities[4]

Which.co.uk Misleading[5]

CVE-2022-38970[6]

Suggest an edit to this article

Cybersecurity Knowledge Base

Latest InfoSec News

Cybersecurity Academy

Go to Homepage

Stay informed of the latest Cybersecurity trends, threats and developments. Sign up for our Weekly Cybersecurity Newsletter Today.

Remember, *CyberSecurity Starts With You!*

- Email is responsible for around **94% of all malware**.
- **Every 39 seconds,** there is a new attack somewhere on the web.
- An average of **around 24,000 malicious mobile apps** are blocked daily on the internet.

Bookmark

RiSec.N0tst3

Share the word, let's increase Cybersecurity Awareness as we know it

No related articles.

← Previous Post

Next Post →

Pingback: ieGeek Vulnerabilities still prevalent in 2022 - Amazon Ft. IG20

Pingback: ieGeek Vulnerabilities still prevalent in 2022 – OasisNews

Pingback: ieGeek Vulnerabilities Still Prevalent In 2022 - ThreatsHub Cybersecurity News

Pingback: IoT Devices That make Security Pros Cringe

Leave a Comment

Your email address will not be published. Required fields are marked *

Type here..

Name*

E-mail*

Website

Save my name, email, and website in this browser for the next time I comment.

RiSec Captcha + 87 = 91

Post Comment »