



# CVE-2022-2675

Published on: Not Yet Published

Last Modified on: 08/11/2022 03:28:00 PM UTC

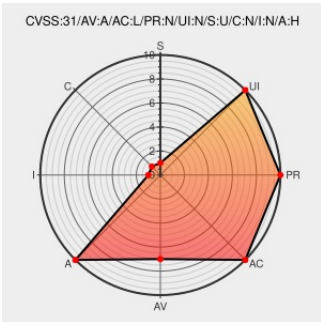
## CVE-2022-2675 - advisory for

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Go 1](#) from [Unitree](#) contain the following vulnerability:

Using off-the-shelf commodity hardware, the Unitree Go 1 robotics platform version H0.1.7 and H0.1.9 (using firmware version 0.1.35) can be powered down by an attacker within normal RF range without authentication. Other versions may be affected, such as the A1.

CVE-2022-2675 has been assigned by [cve@rapid7.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [Unitree](#) - **Go 1** version  $\leq$  **0.1.35**

Affected Vendor/Software: [Unitree](#) - **Go 1** version  $<$  **0.1.35**

CVSS3 Score: **6.5 - MEDIUM**

| Attack Vector           | Attack Complexity      | Privileges Required | User Interaction    |
|-------------------------|------------------------|---------------------|---------------------|
| <b>ADJACENT_NETWORK</b> | <b>LOW</b>             | <b>NONE</b>         | <b>NONE</b>         |
| Scope                   | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b>        | <b>NONE</b>            | <b>NONE</b>         | <b>HIGH</b>         |

## CVE References

| Description   | Tags   | Link   |
|---|--|--|
| KF on Twitter: "Good news! Remember that robot dog you saw with a gun!? It was made by @UnitreeRobotics. Seems all you need to dump it in the dirt is @flipper_zero. The PDB has a 433mhz backdoor. No need for @gnuradio! <a href="https://t.co/xjDepcGYe2">https://t.co/xjDepcGYe2</a> cc/ @UnitreeRobot007 @IrvingRobotics @shunweicapital <a href="https://t.co/6PJHjcsjJL">https://t.co/6PJHjcsjJL</a> " / Twitter | <a href="#">nitter.domain.glass</a><br><a href="#">text/html</a> | <a href="https://twitter.com/d0tslash/status/1555326302462394370">MISC twitter.com/d0tslash/status/1555326302462394370</a> |

application/pdf

www.mybotshop.de/Datasheet/Unitree\_A1\_User\_Manual\_v1.0.pdf

Just a moment...

fccid.io

text/html

Inactive Link Not Archived

MISC fccid.io/2A5PE-YUSHU001/Users-Manual/User-Manual-5810729

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

### Known Affected Configurations (CPE V2.3)

| Type             | Vendor  | Product       | Version | Update | Edition | Language |
|------------------|---------|---------------|---------|--------|---------|----------|
| Hardware         | Unitree | Go 1          | h0.1.7  | All    | All     | All      |
| Hardware         | Unitree | Go 1          | h0.1.9  | All    | All     | All      |
| Operating System | Unitree | Go 1 Firmware | All     | All    | All     | All      |
| Operating System | Unitree | Go 1 Firmware | All     | All    | All     | All      |

cpe:2.3:h:unitree:go\_1:h0.1.7:\*:\*:\*:\*:\*:

cpe:2.3:h:unitree:go\_1:h0.1.9:\*:\*:\*:\*:\*:

cpe:2.3:o:unitree:go\_1\_firmware:\*:\*:\*:\*:\*:

cpe:2.3:o:unitree:go\_1\_firmware:\*:\*:\*:\*:\*:

### Discovery Credit

Discovered and reported by security researcher Kevin Finisterre

### Social Mentions

| Source     | Title  | Posted (UTC)        |
|------------|--|---------------------|
| @CVEreport | CVE-2022-2675 : Using off-the-shelf commodity hardware, the Unitree Go 1 robotics platform version H0.1.7 and H0.1.... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a> | 2022-08-05 17:10:24 |
| /r/netcve  | <a href="#">CVE-2022-2675</a>  | 2022-08-05 18:38:47 |

[← Previous ID](#)

[Next ID →](#)

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**