



# CVE-2018-5402

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2018-5402  |
| <b>State</b>           | PUBLIC   |
| <b>Assigner</b>        | cert@cert.org  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2018-10-08 15:29:00 UTC  |
| <b>Updated</b>         | 2019-10-09 23:41:00 UTC  |
| <b>Description</b>     | The Auto-Maskin DCU 210E, RP-210E, and Marine Pro Observer Android App use an embedded webserver that uses un... |

## Risk And Classification

**Problem Types:** CWE-310

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                      | Product                             | Version | Update | Edition | Language |
|------------------|-----------------------------|-------------------------------------|---------|--------|---------|----------|
| Hardware         | <a href="#">Arm</a>         | <a href="#">Arm7</a>                | All     | All    | All     | All      |
| Hardware         | <a href="#">Arm</a>         | <a href="#">Arm7</a>                | All     | All    | All     | All      |
| Hardware         | <a href="#">Auto-maskin</a> | <a href="#">Dcu 210e</a>            | -       | All    | All     | All      |
| Hardware         | <a href="#">Auto-maskin</a> | <a href="#">Dcu 210e</a>            | -       | All    | All     | All      |
| Operating System | <a href="#">Auto-maskin</a> | <a href="#">Dcu 210e Firmware</a>   | -       | All    | All     | All      |
| Operating System | <a href="#">Auto-maskin</a> | <a href="#">Dcu 210e Firmware</a>   | -       | All    | All     | All      |
| Application      | <a href="#">Auto-maskin</a> | <a href="#">Marine Pro Observer</a> | -       | All    | All     | All      |
| Application      | <a href="#">Auto-maskin</a> | <a href="#">Marine Pro Observer</a> | -       | All    | All     | All      |
| Hardware         | <a href="#">Auto-maskin</a> | <a href="#">Rp 210e</a>             | -       | All    | All     | All      |
| Hardware         | <a href="#">Auto-maskin</a> | <a href="#">Rp 210e</a>             | -       | All    | All     | All      |
| Operating System | <a href="#">Auto-maskin</a> | <a href="#">Rp 210e Firmware</a>    | -       | All    | All     | All      |
| Operating System | <a href="#">Auto-maskin</a> | <a href="#">Rp 210e Firmware</a>    | -       | All    | All     | All      |

## References

| Reference   | Source  | Link   | Tags                     |
|---|---------|--|--------------------------|
| CERT Vulnerability Notes Database   | CERT-VN | <a href="http://www.kb.cert.org">www.kb.cert.org</a> | Third Party Advisory, US |
| Auto-Maskin RP210E, DCU210E, and Marine Observer Pro (Android App)   CISA | MISC    | <a href="http://www.us-cert.gov">www.us-cert.gov</a> |                          |

|                          |         |  |                     |
|--------------------------|---------|--|---------------------|
| CVE Program record       | CVE.ORG | <a href="http://www.cve.org">www.cve.org</a>   | canonical           |
| NVD vulnerability detail | NVD     | <a href="http://nvd.nist.gov">nvd.nist.gov</a> | canonical, analysis |

**Vendor Comments And Credit**

Discovery Credit

**LEGACY:** Reporters: Brian Satira, Brian Olson, Organization: Project Gunsway

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](http://CVE.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This 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](http://The MITRE Corporation) and the authoritative source of CVE content is [MITRE's CVE web site](http://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](http://status.cve.report)