



# CVE-2020-9200

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

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2020-9200   |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | psirt@huawei.com  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2020-12-24 16:15:00 UTC   |
| <b>Updated</b>         | 2020-12-28 19:23:00 UTC   |
| <b>Description</b>     | There has a CSV injection vulnerability in iManager NetEco 6000 versions V600R021C00. An attacker with common privilege |

## Risk And Classification

**Problem Types:** CWE-1236

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                 | Product                              | Version     | Update | Edition | Language |
|-------------|------------------------|--------------------------------------|-------------|--------|---------|----------|
| Application | <a href="#">Huawei</a> | <a href="#">Imanager Neteco 6000</a> | v600r021c00 | All    | All     | All      |
| Application | <a href="#">Huawei</a> | <a href="#">Imanager Neteco 6000</a> | v600r021c00 | All    | All     | All      |

## References

| Reference  | Source  | Link   | Tags                |
|--|---------|--|---------------------|
| Security Advisory - CSV Injection Vulnerability in iManager NetEco Product | MISC    | <a href="http://www.huawei.com">www.huawei.com</a> | Vendor Advisory     |
| 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 |

No vendor comments have been submitted for this CVE.

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

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](#)**