



CVE-2020-25189

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2020-25189 |
| State | PUBLIC |
| Assigner | ics-cert@hq.dhs.gov |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2020-11-21 17:15:00 UTC |
| Updated | 2020-12-03 15:52:00 UTC |
| Description | The affected product is vulnerable to three stack-based buffer overflows, which may allow an unauthenticated attacker to re |

Risk And Classification

Problem Types: CWE-121

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|-------------------------|--------------------------------|---------|--------|---------|----------|
| Hardware | Paradox | Ip150 | - | All | All | All |
| Hardware | Paradox | Ip150 | - | All | All | All |
| Operating System | Paradox | Ip150 Firmware | 5.02.09 | All | All | All |
| Operating System | Paradox | Ip150 Firmware | 5.02.09 | All | All | All |

References

| Reference | Source | Link | Tags |
|--------------------------|---------|---|--|
| Paradox IP150 CISA | MISC | us-cert.cisa.gov | Third Party Advisory, US Government Resource |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

No vendor comments have been submitted for this CVE.

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

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](#) 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](#)