



CVE-2017-5255

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2017-5255 |
| State | PUBLIC |
| Assigner | cve@rapid7.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2017-12-20 22:29:00 UTC |
| Updated | 2019-10-09 23:28:00 UTC |
| Description | In version 3.5 and prior of Cambium Networks ePMP firmware, a lack of input sanitation for certain parameters on the web |

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|---------------------------------|------------------------------------|---------|--------|---------|----------|
| Hardware | Cambiumnetworks | Epmp 1000 | - | All | All | All |
| Hardware | Cambiumnetworks | Epmp 1000 | - | All | All | All |
| Operating System | Cambiumnetworks | Epmp 1000 Firmware | All | All | All | All |
| Hardware | Cambiumnetworks | Epmp 2000 | - | All | All | All |
| Hardware | Cambiumnetworks | Epmp 2000 | - | All | All | All |
| Operating System | Cambiumnetworks | Epmp 2000 Firmware | All | All | All | All |

References

| Reference | Source | Link | Tag |
|--|------------|--|------|
| Cambium ePMP1000 - 'get_chart' Shell via Command Injection (Metasploit) - CGI remote Exploit | EXPLOIT-DB | www.exploit-db.com | This |
| R7-2017-25: Cambium ePMP and cnPilot Multiple Vulnerabilities | MISC | blog.rapid7.com | This |
| CVE Program record | CVE.ORG | www.cve.org | car |
| NVD vulnerability detail | NVD | nvd.nist.gov | car |

No vendor comments have been submitted for this CVE.

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

© [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](#) 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](#)