



CVE-2023-1205

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2023-1205 |
| State | PUBLIC |
| Assigner | vulnreport@tenable.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2023-03-10 18:15:00 UTC |
| Updated | 2023-03-15 17:54:00 UTC |
| Description | NETGEAR Nighthawk WiFi6 Router prior to V1.0.10.94 is vulnerable to cross-site request forgery attacks on all endpoints c |

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|-------------------------|--------------------------------|---------|--------|---------|----------|
| Hardware | Netgear | Rax30 | - | All | All | All |
| Operating System | Netgear | Rax30 Firmware | All | All | All | All |

References

| Reference | Source | Link | Tags |
|---|---------|------------------------------|---------------------|
| Netgear RAX30 Multiple Vulnerabilities - Research Advisory Tenable® | MISC | tenable.com | |
| 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.

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report