



CVE-2020-5533

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

Summary

| | |
|------------------------|------------------------------------------------------------------------------------------------------------------------------|
| CVE | CVE-2020-5533 |
| State | PUBLIC |
| Assigner | vultures@jpcert.or.jp |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2020-02-21 10:15:00 UTC |
| Updated | 2020-02-21 17:16:00 UTC |
| Description | Cross-site scripting vulnerability in Aterm WG2600HS firmware Ver1.3.2 and earlier allows remote attackers to inject arbitra |

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|--------|-----------------------------------------|---------|--------|---------|----------|
| Hardware | Nec | Aterm Wg2600hs | - | All | All | All |
| Hardware | Nec | Aterm Wg2600hs | - | All | All | All |
| Operating System | Nec | Aterm Wg2600hs Firmware | All | All | All | All |

References

| Reference | Source | Link | Tags |
|----------------------------------------------------------|---------|------------------------------|----------------------|
| JVN#49410695: Multiple vulnerabilities in Aterm WG2600HS | MISC | jvn.jp | Third Party Advisory |
| NV20-003: セキュリティ情報 NEC | MISC | jpn.nec.com | Third Party Advisory |
| 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