



CVE-2021-39290

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2021-39290 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2021-08-23 05:15:00 UTC |
| Updated | 2023-11-02 15:48:00 UTC |
| Description | Certain NetModule devices allow Limited Session Fixation via PHPSESSID. These models with firmware before 4.3.0.113, |

Risk And Classification

Problem Types: CWE-384

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|---------------------------|---------------------------------|---------|--------|---------|----------|
| Hardware | Netmodule | Nb1600 | - | All | All | All |
| Operating System | Netmodule | Nb1600 Firmware | All | All | All | All |
| Hardware | Netmodule | Nb1601 | - | All | All | All |
| Operating System | Netmodule | Nb1601 Firmware | All | All | All | All |
| Hardware | Netmodule | Nb1800 | - | All | All | All |
| Operating System | Netmodule | Nb1800 Firmware | All | All | All | All |
| Hardware | Netmodule | Nb1810 | - | All | All | All |
| Operating System | Netmodule | Nb1810 Firmware | All | All | All | All |
| Hardware | Netmodule | Nb2700 | - | All | All | All |
| Operating System | Netmodule | Nb2700 Firmware | All | All | All | All |
| Hardware | Netmodule | Nb2710 | - | All | All | All |
| Operating System | Netmodule | Nb2710 Firmware | All | All | All | All |
| Hardware | Netmodule | Nb2800 | - | All | All | All |
| Operating System | Netmodule | Nb2800 Firmware | All | All | All | All |
| Hardware | Netmodule | Nb2810 | - | All | All | All |
| Operating System | Netmodule | Nb2810 Firmware | All | All | All | All |
| Hardware | Netmodule | Nb3700 | - | All | All | All |

| | | | | | | |
|------------------|---------------------------|---|-----|-----|-----|-----|
| Operating System | Netmodule | Nb3700 Firmware | All | All | All | All |
| Hardware | Netmodule | Nb3701 | - | All | All | All |
| Operating System | Netmodule | Nb3701 Firmware | All | All | All | All |
| Hardware | Netmodule | Nb3710 | - | All | All | All |
| Operating System | Netmodule | Nb3710 Firmware | All | All | All | All |
| Hardware | Netmodule | Nb3711 | - | All | All | All |
| Operating System | Netmodule | Nb3711 Firmware | All | All | All | All |
| Hardware | Netmodule | Nb3720 | - | All | All | All |
| Operating System | Netmodule | Nb3720 Firmware | All | All | All | All |
| Hardware | Netmodule | Nb3800 | - | All | All | All |
| Operating System | Netmodule | Nb3800 Firmware | All | All | All | All |
| Hardware | Netmodule | Nb800 | - | All | All | All |
| Operating System | Netmodule | Nb800 Firmware | All | All | All | All |
| Application | Netmodule | Netmodule Router Software | All | All | All | All |

References

| Reference | Source | Link |
|---|---------|--|
| NetModule Robust Communication | MISC | www.netmodule.com |
| Full Disclosure: SEC Consult SA-20210820-0 :: Multiple Vulnerabilities in NetModule Router Software | MISC | seclists.org |
| CVE Program record | CVE.ORG | www.cve.org |
| NVD vulnerability detail | NVD | nvd.nist.gov |

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