



# CVE-2002-2159

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2002-2159  |
| <b>State</b>           | PUBLIC   |
| <b>Assigner</b>        | cve@mitre.org  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2002-12-31 05:00:00 UTC  |
| <b>Updated</b>         | 2017-07-12 01:29:00 UTC  |
| <b>Description</b>     | Linksys EtherFast Cable/DSL BEFSR11, BEFSR41 and BEFSRU31 with the firmware 1.42.7 upgrade installed opens TCP |

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

| Type     | Vendor                  | Product                 | Version | Update | Edition | Language |
|----------|-------------------------|-------------------------|---------|--------|---------|----------|
| Hardware | <a href="#">Linksys</a> | <a href="#">Befsr11</a> | 1.42.7  | All    | All     | All      |
| Hardware | <a href="#">Linksys</a> | <a href="#">Befsr11</a> | 1.42.7  | All    | All     | All      |
| Hardware | <a href="#">Linksys</a> | <a href="#">Befsr41</a> | 1.42.7  | All    | All     | All      |
| Hardware | <a href="#">Linksys</a> | <a href="#">Befsr41</a> | 1.42.7  | All    | All     | All      |
| Hardware | <a href="#">Linksys</a> | <a href="#">Befsr31</a> | 1.42.7  | All    | All     | All      |
| Hardware | <a href="#">Linksys</a> | <a href="#">Befsr31</a> | 1.42.7  | All    | All     | All      |

## References

### Reference

Sorry, the content you are trying to view does not exist. If you feel this message is in error, please email the webmaster.

ISS X-Force Database: linksys-etherfast-admin-enabled (9330): Linksys EtherFast routers enable remote administration upon firmware upgrade

'Linksys Cable/DSL 4port Exposure Issue' - SecuriTeam

CVE Program record

NVD vulnerability detail

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](#)**