



CVE-2011-1547

Published on: 05/09/2011 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:16 PM UTC

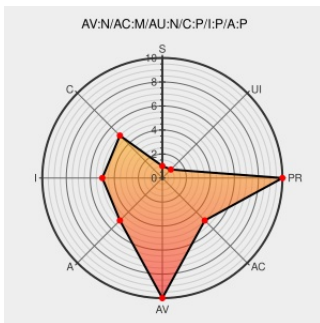
CVE-2011-1547

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Netbsd](#) from [Netbsd](#) contain the following vulnerability:

Multiple stack consumption vulnerabilities in the kernel in NetBSD 4.0, 5.0 before 5.0.3, and 5.1 before 5.1.1, when IPsec is enabled, allow remote attackers to cause a denial of service (memory corruption and panic) or possibly have unspecified other impact via a crafted (1) IPv4 or (2) IPv6 packet with nested IPComp headers.

CVE-2011-1547 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **6.8 - MEDIUM**

Access Vector

NETWORK

Access Complexity

MEDIUM

Authentication

NONE

Confidentiality Impact

PARTIAL

Integrity Impact

PARTIAL

Availability Impact

PARTIAL

CVE References

Description

Tags

Link

[Vendor Advisory](#)

[ftp.netbsd.org](#)

[text/plain](#)

[NETBSD NetBSD-SA2011-004](#)

[Full-disclosure] BSD derived RFC3173 IPComp encapsulation will expand arbitrarily nested payload

[lists.grok.org.uk](#)

[text/x-c](#)

[Inactive Link](#) [Not Archived](#)

[FULLDISC 20110401 BSD derived RFC3173 IPComp encapsulation will expand arbitrarily nested payload](#)

US-CERT Vulnerability Note VU#668220 - IPComp encapsulation nested payload vulnerability

[US Government Resource](#)

[www.kb.cert.org](#)

[text/html](#)

[CERT-VN VU#668220](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further,

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Netbsd	Netbsd	4.0	All	All	All
Operating System	Netbsd	Netbsd	5.0	All	All	All
Operating System	Netbsd	Netbsd	5.0.1	All	All	All
Operating System	Netbsd	Netbsd	5.0.2	All	All	All
Operating System	Netbsd	Netbsd	5.1	All	All	All
Operating System	Netbsd	Netbsd	4.0	All	All	All
Operating System	Netbsd	Netbsd	5.0	All	All	All
Operating System	Netbsd	Netbsd	5.0.1	All	All	All
Operating System	Netbsd	Netbsd	5.0.2	All	All	All
Operating System	Netbsd	Netbsd	5.1	All	All	All
cpe:2.3:o:netbsd:netbsd:4.0:*****:						
cpe:2.3:o:netbsd:netbsd:5.0:*****:						
cpe:2.3:o:netbsd:netbsd:5.0.1:*****:						
cpe:2.3:o:netbsd:netbsd:5.0.2:*****:						
cpe:2.3:o:netbsd:netbsd:5.1:*****:						
cpe:2.3:o:netbsd:netbsd:4.0:*****:						
cpe:2.3:o:netbsd:netbsd:5.0:*****:						
cpe:2.3:o:netbsd:netbsd:5.0.1:*****:						
cpe:2.3:o:netbsd:netbsd:5.0.2:*****:						
cpe:2.3:o:netbsd:netbsd:5.1:*****:						

No vendor comments have been submitted for this CVE

© [CVE.report](#) 2023   |

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](#)