

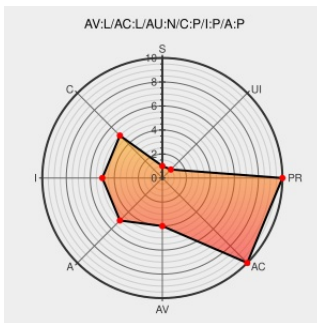


CVE-2002-1476

Published on: 04/22/2003 04:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:01 PM UTC

CVE-2002-1476

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

Buffer overflow in setlocale in libc on NetBSD 1.4.x through 1.6, and possibly other operating systems, when called with the LC_ALL category, allows local attackers to execute arbitrary code via a user-controlled locale string that has more than 6 elements, which exceeds the boundaries of the new_categories category array, as exploitable through programs such as xterm and zsh.

CVE-2002-1476 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.6 - MEDIUM**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

ISS X-Force Database: netbsd-libc-setlocale-bo (10159): NetBSD X11 libc setlocale() buffer overflow

Tags

[Patch](#)
[Vendor Advisory](#)
[web.archive.org](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

Link

[XF netbsd-libc-setlocale-bo\(10159\)](#)

No Description Provided

[www.osvdb.org](#)

[OSVDB 7565](#)

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

[ftp.netbsd.org](#)
[text/plain](#)

[NETBSD NetBSD-SA2002-012](#)

NetBSD libc Setlocale Buffer Overflow Vulnerability

[Patch](#)

[BID 5724](#)

comment@cve.report

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	1.4	All	All	All
Operating System	Netbsd	Netbsd	1.5	All	All	All
Operating System	Netbsd	Netbsd	1.5.1	All	All	All
Operating System	Netbsd	Netbsd	1.5.2	All	All	All
Operating System	Netbsd	Netbsd	1.5.3	All	All	All
Operating System	Netbsd	Netbsd	1.6	beta	All	All
Operating System	Netbsd	Netbsd	1.4	All	All	All
Operating System	Netbsd	Netbsd	1.5	All	All	All
Operating System	Netbsd	Netbsd	1.5.1	All	All	All
Operating System	Netbsd	Netbsd	1.5.2	All	All	All
Operating System	Netbsd	Netbsd	1.5.3	All	All	All
Operating System	Netbsd	Netbsd	1.6	beta	All	All
cpe:2.3:o:netbsd:netbsd:1.4:*:*:*:*:*:						
cpe:2.3:o:netbsd:netbsd:1.5:*:*:*:*:*:						
cpe:2.3:o:netbsd:netbsd:1.5.1:*:*:*:*:*:						
cpe:2.3:o:netbsd:netbsd:1.5.2:*:*:*:*:*:						
cpe:2.3:o:netbsd:netbsd:1.5.3:*:*:*:*:*:						
cpe:2.3:o:netbsd:netbsd:1.6:beta:*:*:*:*:						

cpe:2.3:o:netbsd:netbsd:1.4.*.*.*.*.*.*.*.*
cpe:2.3:o:netbsd:netbsd:1.5.*.*.*.*.*.*.*.*
cpe:2.3:o:netbsd:netbsd:1.5.1.*.*.*.*.*.*.*.*
cpe:2.3:o:netbsd:netbsd:1.5.2.*.*.*.*.*.*.*.*
cpe:2.3:o:netbsd:netbsd:1.5.3.*.*.*.*.*.*.*.*
cpe:2.3:o:netbsd:netbsd:1.6:beta.*.*.*.*.*.*.*.*

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© 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