

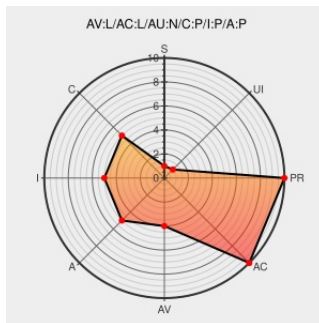


CVE-2002-0973

Published on: 08/23/2002 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:04 PM UTC

CVE-2002-0973

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

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

Integer signedness error in several system calls for FreeBSD 4.6.1 RELEASE-p10 and earlier may allow attackers to access sensitive kernel memory via large negative values to the (1) accept, (2) getsockname, and (3) getpeername system calls, and the (4) vesa FBIO_GETPALETTE ioctl.

CVE-2002-0973 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

Tags

Link

FreeBSD System Call Signed Integer Buffer Overflow Vulnerability

[cve.report \(archive\)](#)
[text/html](#)

[🌐](#) [BID 5493](#)

ISS X-Force Database: freebsd-negative-system-call-bo (9903): FreeBSD negative argument system call buffer overflow could return sensitive information

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

[🌐](#) [XF freebsd-negative-system-call-bo\(9903\)](#)

'FreeBSD Security Advisory FreeBSD-SA-02:38.signed-error' - MARC

[marc.info](#)
[text/html](#)

[🌐](#) [FREEBSD FreeBSD-SA-02:38](#)

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	Freebsd	Freebsd	4.0	All	All	All
Operating System	Freebsd	Freebsd	4.1	All	All	All
Operating System	Freebsd	Freebsd	4.1.1	All	All	All
Operating System	Freebsd	Freebsd	4.1.1	release	All	All
Operating System	Freebsd	Freebsd	4.1.1	stable	All	All
Operating System	Freebsd	Freebsd	4.2	All	All	All
Operating System	Freebsd	Freebsd	4.2	stable	All	All
Operating System	Freebsd	Freebsd	4.3	All	All	All
Operating System	Freebsd	Freebsd	4.3	release	All	All
Operating System	Freebsd	Freebsd	4.3	stable	All	All
Operating System	Freebsd	Freebsd	4.4	All	All	All
Operating System	Freebsd	Freebsd	4.4	stable	All	All
Operating System	Freebsd	Freebsd	4.5	All	All	All
Operating System	Freebsd	Freebsd	4.5	release	All	All
Operating System	Freebsd	Freebsd	4.5	stable	All	All
Operating System	Freebsd	Freebsd	4.6	All	All	All
Operating System	Freebsd	Freebsd	4.6	release	All	All
Operating System	Freebsd	Freebsd	4.6.1	release_p10	All	All
Operating System	Freebsd	Freebsd	4.0	All	All	All


```
cpe:2.3:0:freebsd:freebsd:4.3: : : : : :
```

```
cpe:2.3:o:freebsd:freebsd:4.3:release:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.3:stable:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.4:*:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.4:stable:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.5:.*:.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:o:freebsd:freebsd:4.5:release:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.5:stable:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.6:*:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.6:release:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.6.1:release p10:::~::~:
```

```
cpe:2.3:o:freebsd:freebsd:4.0:*:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.1:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.1.1:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.1.1:release:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.1.1:stable:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.2:*:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.2:stable:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.3:*:*:*:*:*:*:
```

```
cpe:2.3:0:freebsd:freebsd:4.3:release:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.3:stable:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.4:*:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.4:stable:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.5:*:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.5:release:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.5:stable:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.6:*:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.6:release:*:*:*:*:*:
```

```
cpe:2.3:o:freebsd:freebsd:4.6.1:release_p10:*:*:*:*:*:
```

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](#)