



CVE-2002-1976

Published on: 12/31/2002 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:02 PM UTC

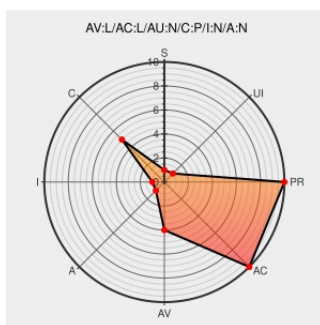
CVE-2002-1976

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

ifconfig, when used on the Linux kernel 2.2 and later, does not report when the network interface is in promiscuous mode if it was put in promiscuous mode using PACKET_MR_PROMISC, which could allow attackers to sniff the network without detection, as demonstrated using libpcap.

CVE-2002-1976 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **2.1 - LOW**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

NONE

Availability
Impact

NONE

CVE References

Description

Tags

Link

SecurityFocus HOME Mailing List: BugTraq

[web.archive.org](#)

[text/html](#)

Inactive Link

Not Archived

[BUGTRAQ 20020725](#)
Re: Interface promiscuity
obscurity in Linux

SecurityFocus

[web.archive.org](#)

[text/html](#)

Inactive Link

Not Archived

[BUGTRAQ 20020724](#)
Re: Interface promiscuity
obscurity in Linux

No Description Provided

[web.archive.org](#)

[text/html](#)

Inactive Link

Not Archived

[BUGTRAQ 20020724](#)
Interface promiscuity
obscurity in Linux

ISS X-Force Database: linux-ifconfig-promiscuous-mode (9676): Linux kernel ifconfig could fail to show that a network interface is in promiscuous mode

[web.archive.org](#)

[text/html](#)

Inactive Link

Not Archived

[XF linux-ifconfig-](#)
[promiscuous-](#)
[mode\(9676\)](#)

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, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to 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	Linux	Linux Kernel	2.2.0	All	All	All
Operating System	Linux	Linux Kernel	2.2.1	All	All	All
Operating System	Linux	Linux Kernel	2.2.10	All	All	All
Operating System	Linux	Linux Kernel	2.2.11	All	All	All
Operating System	Linux	Linux Kernel	2.2.12	All	All	All
Operating System	Linux	Linux Kernel	2.2.13	All	All	All
Operating System	Linux	Linux Kernel	2.2.14	All	All	All
Operating System	Linux	Linux Kernel	2.2.15	All	All	All
Operating System	Linux	Linux Kernel	2.2.16	All	All	All
Operating System	Linux	Linux Kernel	2.2.17	All	All	All
Operating System	Linux	Linux Kernel	2.2.18	All	All	All
Operating System	Linux	Linux Kernel	2.2.19	All	All	All
Operating System	Linux	Linux Kernel	2.2.2	All	All	All
Operating System	Linux	Linux Kernel	2.2.20	All	All	All
Operating System	Linux	Linux Kernel	2.2.3	All	All	All
Operating System	Linux	Linux Kernel	2.2.4	All	All	All
Operating System	Linux	Linux Kernel	2.2.5	All	All	All

System						
Operating System	Linux	Linux Kernel	2.2.6	All	All	All
Operating System	Linux	Linux Kernel	2.2.7	All	All	All
Operating System	Linux	Linux Kernel	2.2.8	All	All	All
Operating System	Linux	Linux Kernel	2.2.9	All	All	All
Operating System	Linux	Linux Kernel	2.3.0	All	All	All
Operating System	Linux	Linux Kernel	2.3.99	All	All	All
Operating System	Linux	Linux Kernel	2.4.0	All	All	All
Operating System	Linux	Linux Kernel	2.4.1	All	All	All
Operating System	Linux	Linux Kernel	2.4.10	All	All	All
Operating System	Linux	Linux Kernel	2.4.11	All	All	All
Operating System	Linux	Linux Kernel	2.4.12	All	All	All
Operating System	Linux	Linux Kernel	2.4.13	All	All	All
Operating System	Linux	Linux Kernel	2.4.14	All	All	All
Operating System	Linux	Linux Kernel	2.4.15	All	All	All
Operating System	Linux	Linux Kernel	2.4.16	All	All	All
Operating System	Linux	Linux Kernel	2.4.17	All	All	All
Operating System	Linux	Linux Kernel	2.4.18	All	All	All
Operating System	Linux	Linux Kernel	2.4.18	All	x86	All
Operating System	Linux	Linux Kernel	2.4.19	pre1	All	All
Operating System	Linux	Linux Kernel	2.4.19	pre2	All	All
Operating System	Linux	Linux Kernel	2.4.19	pre3	All	All
Operating System	Linux	Linux Kernel	2.4.19	pre4	All	All
Operating System	Linux	Linux Kernel	2.4.19	pre5	All	All

Operating System	Linux	Linux Kernel	Linux	proc	All	All
Operating System	Linux	Linux Kernel	2.4.19	pre6	All	All
Operating System	Linux	Linux Kernel	2.4.2	All	All	All
Operating System	Linux	Linux Kernel	2.4.3	All	All	All
Operating System	Linux	Linux Kernel	2.4.4	All	All	All
Operating System	Linux	Linux Kernel	2.4.5	All	All	All
Operating System	Linux	Linux Kernel	2.4.6	All	All	All
Operating System	Linux	Linux Kernel	2.4.7	All	All	All
Operating System	Linux	Linux Kernel	2.4.8	All	All	All
Operating System	Linux	Linux Kernel	2.4.9	All	All	All
Operating System	Linux	Linux Kernel	2.2.0	All	All	All
Operating System	Linux	Linux Kernel	2.2.1	All	All	All
Operating System	Linux	Linux Kernel	2.2.10	All	All	All
Operating System	Linux	Linux Kernel	2.2.11	All	All	All
Operating System	Linux	Linux Kernel	2.2.12	All	All	All
Operating System	Linux	Linux Kernel	2.2.13	All	All	All
Operating System	Linux	Linux Kernel	2.2.14	All	All	All
Operating System	Linux	Linux Kernel	2.2.15	All	All	All
Operating System	Linux	Linux Kernel	2.2.16	All	All	All
Operating System	Linux	Linux Kernel	2.2.17	All	All	All
Operating System	Linux	Linux Kernel	2.2.18	All	All	All
Operating System	Linux	Linux Kernel	2.2.19	All	All	All
Operating System	Linux	Linux Kernel	2.2.2	All	All	All
Operating System	Linux	Linux Kernel	2.2.20	All	All	All

Operating System	Linux	Linux Kernel	2.2.20	All	All	All
Operating System	Linux	Linux Kernel	2.2.3	All	All	All
Operating System	Linux	Linux Kernel	2.2.4	All	All	All
Operating System	Linux	Linux Kernel	2.2.5	All	All	All
Operating System	Linux	Linux Kernel	2.2.6	All	All	All
Operating System	Linux	Linux Kernel	2.2.7	All	All	All
Operating System	Linux	Linux Kernel	2.2.8	All	All	All
Operating System	Linux	Linux Kernel	2.2.9	All	All	All
Operating System	Linux	Linux Kernel	2.3.0	All	All	All
Operating System	Linux	Linux Kernel	2.3.99	All	All	All
Operating System	Linux	Linux Kernel	2.4.0	All	All	All
Operating System	Linux	Linux Kernel	2.4.1	All	All	All
Operating System	Linux	Linux Kernel	2.4.10	All	All	All
Operating System	Linux	Linux Kernel	2.4.11	All	All	All
Operating System	Linux	Linux Kernel	2.4.12	All	All	All
Operating System	Linux	Linux Kernel	2.4.13	All	All	All
Operating System	Linux	Linux Kernel	2.4.14	All	All	All
Operating System	Linux	Linux Kernel	2.4.15	All	All	All
Operating System	Linux	Linux Kernel	2.4.16	All	All	All
Operating System	Linux	Linux Kernel	2.4.17	All	All	All
Operating System	Linux	Linux Kernel	2.4.18	All	All	All
Operating System	Linux	Linux Kernel	2.4.18	All	x86	All
Operating System	Linux	Linux Kernel	2.4.19	pre1	All	All
Operating System	Linux	Linux Kernel	2.4.19	pre1	All	All

Operating System	Linux	Linux Kernel	2.4.19	pre2	All	All
Operating System	Linux	Linux Kernel	2.4.19	pre3	All	All
Operating System	Linux	Linux Kernel	2.4.19	pre4	All	All
Operating System	Linux	Linux Kernel	2.4.19	pre5	All	All
Operating System	Linux	Linux Kernel	2.4.19	pre6	All	All
Operating System	Linux	Linux Kernel	2.4.2	All	All	All
Operating System	Linux	Linux Kernel	2.4.3	All	All	All
Operating System	Linux	Linux Kernel	2.4.4	All	All	All
Operating System	Linux	Linux Kernel	2.4.5	All	All	All
Operating System	Linux	Linux Kernel	2.4.6	All	All	All
Operating System	Linux	Linux Kernel	2.4.7	All	All	All
Operating System	Linux	Linux Kernel	2.4.8	All	All	All
Operating System	Linux	Linux Kernel	2.4.9	All	All	All
cpe:2.3:o:linux:linux_kernel:2.2.0:*****:						
cpe:2.3:o:linux:linux_kernel:2.2.1:*****:						
cpe:2.3:o:linux:linux_kernel:2.2.10:*****:						
cpe:2.3:o:linux:linux_kernel:2.2.11:*****:						
cpe:2.3:o:linux:linux_kernel:2.2.12:*****:						
cpe:2.3:o:linux:linux_kernel:2.2.13:*****:						
cpe:2.3:o:linux:linux_kernel:2.2.14:*****:						
cpe:2.3:o:linux:linux_kernel:2.2.15:*****:						
cpe:2.3:o:linux:linux_kernel:2.2.16:*****:						
cpe:2.3:o:linux:linux_kernel:2.2.17:*****:						
cpe:2.3:o:linux:linux_kernel:2.2.18:*****:						
cpe:2.3:o:linux:linux_kernel:2.2.19:*****:						
cpe:2.3:o:linux:linux_kernel:2.2.2:*****:						

cpe:2.3:o:linux:linux_kernel:2.2.20:****:*:
cpe:2.3:o:linux:linux_kernel:2.2.3:****:*:
cpe:2.3:o:linux:linux_kernel:2.2.4:****:*:
cpe:2.3:o:linux:linux_kernel:2.2.5:****:*:
cpe:2.3:o:linux:linux_kernel:2.2.6:****:*:
cpe:2.3:o:linux:linux_kernel:2.2.7:****:*:
cpe:2.3:o:linux:linux_kernel:2.2.8:****:*:
cpe:2.3:o:linux:linux_kernel:2.2.9:****:*:
cpe:2.3:o:linux:linux_kernel:2.3.0:****:*:
cpe:2.3:o:linux:linux_kernel:2.3.99:****:*:
cpe:2.3:o:linux:linux_kernel:2.4.0:****:*:
cpe:2.3:o:linux:linux_kernel:2.4.1:****:*:
cpe:2.3:o:linux:linux_kernel:2.4.10:****:*:
cpe:2.3:o:linux:linux_kernel:2.4.11:****:*:
cpe:2.3:o:linux:linux_kernel:2.4.12:****:*:
cpe:2.3:o:linux:linux_kernel:2.4.13:****:*:
cpe:2.3:o:linux:linux_kernel:2.4.14:****:*:
cpe:2.3:o:linux:linux_kernel:2.4.15:****:*:
cpe:2.3:o:linux:linux_kernel:2.4.16:****:*:
cpe:2.3:o:linux:linux_kernel:2.4.17:****:*:
cpe:2.3:o:linux:linux_kernel:2.4.18:****:*:
cpe:2.3:o:linux:linux_kernel:2.4.18:*x86:****:
cpe:2.3:o:linux:linux_kernel:2.4.19:pre1:****:*:
cpe:2.3:o:linux:linux_kernel:2.4.19:pre2:****:*:
cpe:2.3:o:linux:linux_kernel:2.4.19:pre3:****:*:
cpe:2.3:o:linux:linux_kernel:2.4.19:pre4:****:*:
cpe:2.3:o:linux:linux_kernel:2.4.19:pre5:****:*:
cpe:2.3:o:linux:linux_kernel:2.4.19:pre6:****:*:

cpe:2.3:o:linux:linux_kernel:2.4.2:*****:
cpe:2.3:o:linux:linux_kernel:2.4.3:*****:
cpe:2.3:o:linux:linux_kernel:2.4.4:*****:
cpe:2.3:o:linux:linux_kernel:2.4.5:*****:
cpe:2.3:o:linux:linux_kernel:2.4.6:*****:
cpe:2.3:o:linux:linux_kernel:2.4.7:*****:
cpe:2.3:o:linux:linux_kernel:2.4.8:*****:
cpe:2.3:o:linux:linux_kernel:2.4.9:*****:
cpe:2.3:o:linux:linux_kernel:2.2.0:*****:
cpe:2.3:o:linux:linux_kernel:2.2.1:*****:
cpe:2.3:o:linux:linux_kernel:2.2.10:*****:
cpe:2.3:o:linux:linux_kernel:2.2.11:*****:
cpe:2.3:o:linux:linux_kernel:2.2.12:*****:
cpe:2.3:o:linux:linux_kernel:2.2.13:*****:
cpe:2.3:o:linux:linux_kernel:2.2.14:*****:
cpe:2.3:o:linux:linux_kernel:2.2.15:*****:
cpe:2.3:o:linux:linux_kernel:2.2.16:*****:
cpe:2.3:o:linux:linux_kernel:2.2.17:*****:
cpe:2.3:o:linux:linux_kernel:2.2.18:*****:
cpe:2.3:o:linux:linux_kernel:2.2.19:*****:
cpe:2.3:o:linux:linux_kernel:2.2.2:*****:
cpe:2.3:o:linux:linux_kernel:2.2.20:*****:
cpe:2.3:o:linux:linux_kernel:2.2.3:*****:
cpe:2.3:o:linux:linux_kernel:2.2.4:*****:
cpe:2.3:o:linux:linux_kernel:2.2.5:*****:
cpe:2.3:o:linux:linux_kernel:2.2.6:*****:
cpe:2.3:o:linux:linux_kernel:2.2.7:*****:
cpe:2.3:o:linux:linux_kernel:2.2.8:*****:
cpe:2.3:o:linux:linux_kernel:2.2.9:*****:

```
cpe:2.3.0:linux:linux_kernel:2.2.9: : : : : :
```

```
cpe:2.3:o:linux:linux_kernel:2.3.0:*:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux kernel:2.3.99:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux kernel:2.4.0:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.4.1:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.4.10:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux kernel:2.4.11:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux kernel:2.4.12:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux kernel:2.4.13:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.4.14:*:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux kernel:2.4.15:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux kernel:2.4.16:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux kernel:2.4.17:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux kernel:2.4.18:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.4.18:*:x86:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.4.19:pre1:::~::~:
```

```
cpe:2.3:o:linux:linux kernel:2.4.19:pre2:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.4.19:pre3:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.4.19:pre4:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.4.19:pre5:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux kernel:2.4.19:pre6:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux kernel:2.4.2:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux kernel:2.4.3:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.4.4:*.~*~*~*~*~*~*~*~*~*
```

```
cpe:2.3:o:linux:linux kernel:2.4.5:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux kernel:2.4.6:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.4.7:*:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.4.8:*:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux kernel:2.4.9:*:*:*:*:*:
```

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](#)