



CVE-2002-1574

Published on: 03/03/2004 05:00:00 AM UTC

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

CVE-2002-1574

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

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

Buffer overflow in the ixj telephony card driver in Linux before 2.4.20 has unknown impact and attack vectors.

CVE-2002-1574 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

redhat.com | Red Hat Support

[www.redhat.com](#)
[text/html](#)

[REDHAT RHSA-2004:106](#)

redhat.com | Red Hat Support

[Patch](#)
[Vendor Advisory](#)
[www.redhat.com](#)
[text/html](#)

[REDHAT RHSA-2004:044](#)

redhat.com | Red Hat Support

[www.redhat.com](#)
[text/html](#)

[REDHAT RHSA-2002:206](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
[text/html](#)

[XF linux-ixj-root-privileges\(10417\)](#)

N-096: Red Hat New Kernel Fixes Local Security Issues

[web.archive.org](#)
[text/html](#)

[CIAC N-096](#)

Inactive Link Not Archived

Linux IXJ Telephony Card Driver 2.4 Kernel Privilege Elevation Vulnerability

Patch

Vendor Advisory

cve.report (archive)

text/html

BID 5985

redhat.com | Red Hat Support

www.redhat.com

text/html

REDHAT RHSA-2002:205

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	2.4.1	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	pre1	All	All
Operating System	Linux	Linux Kernel	2.4.18	pre2	All	All
Operating System	Linux	Linux Kernel	2.4.18	pre3	All	All
Operating System	Linux	Linux Kernel	2.4.18	pre4	All	All
Operating System	Linux	Linux Kernel	2.4.18	pre5	All	All

Operating System	Linux	Linux Kernel	2.4.18	pre6	All	All
Operating System	Linux	Linux Kernel	2.4.18	pre7	All	All
Operating System	Linux	Linux Kernel	2.4.18	pre8	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	2.4.1	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	pre1	All	All
Operating System	Linux	Linux Kernel	2.4.18	pre2	All	All

Operating System	Linux	Linux Kernel	2.4.18	pre3	All	All
Operating System	Linux	Linux Kernel	2.4.18	pre4	All	All
Operating System	Linux	Linux Kernel	2.4.18	pre5	All	All
Operating System	Linux	Linux Kernel	2.4.18	pre6	All	All
Operating System	Linux	Linux Kernel	2.4.18	pre7	All	All
Operating System	Linux	Linux Kernel	2.4.18	pre8	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:2.4.1:*****:						
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:pre1:*****:						

```
cpe:2.3:o:linux:linux_kernel:2.4.18:pre2:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.4.18:pre3:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.4.18:pre4:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.4.18:pre5:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.4.18:pre6:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.4.18:pre7:::~::~:
```

```
cpe:2.3:o:linux:linux_kernel:2.4.18:pre8:::~::~:
```

```
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:2.4.1:*:*:*:*:*:*:
```

```
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:pre1:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.4.18:pre2:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.4.18:pre3:*:*:*:*:*:
```

cpe:2.3:o:linux:linux_kernel:2.4.18:pre4:*****:
cpe:2.3:o:linux:linux_kernel:2.4.18:pre5:*****:
cpe:2.3:o:linux:linux_kernel:2.4.18:pre6:*****:
cpe:2.3:o:linux:linux_kernel:2.4.18:pre7:*****:
cpe:2.3:o:linux:linux_kernel:2.4.18:pre8:*****:
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→](#)