



CVE-2002-1572

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

Last Modified on: 06/15/2021 08:10:51 PM UTC

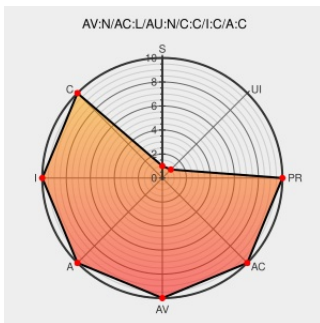
CVE-2002-1572

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

Signed integer overflow in the bttv_read function in the bttv driver (bttv-driver.c) in Linux kernel before 2.4.20 has unknown impact and attack vectors.

CVE-2002-1572 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **10 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

No Description Provided

[linux.bkbits.net](#)

[CONFIRM linux.bkbits.net:8080/linux-2.4/cset@3d6badc0mxsPaOTT_GuPVxCp1_ormw](#)

Inactive Link **Not Archived**

redhat.com | Red Hat
Support

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

[REDHAT RHSA-2002:206](#)

redhat.com | Red Hat
Support

[Patch](#)
[Vendor Advisory](#)
[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

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	2.4.0	All	All	All
Operating System	Linux	Linux Kernel	2.4.0	test1	All	All
Operating System	Linux	Linux Kernel	2.4.0	test10	All	All
Operating System	Linux	Linux Kernel	2.4.0	test11	All	All
Operating System	Linux	Linux Kernel	2.4.0	test12	All	All
Operating System	Linux	Linux Kernel	2.4.0	test2	All	All
Operating System	Linux	Linux Kernel	2.4.0	test3	All	All
Operating System	Linux	Linux Kernel	2.4.0	test4	All	All
Operating System	Linux	Linux Kernel	2.4.0	test5	All	All
Operating System	Linux	Linux Kernel	2.4.0	test6	All	All
Operating System	Linux	Linux Kernel	2.4.0	test7	All	All
Operating System	Linux	Linux Kernel	2.4.0	test8	All	All
Operating System	Linux	Linux Kernel	2.4.0	test9	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	2.4.18	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	2.4.19	All	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
Operating System	Linux	Linux Kernel	2.4.0	All	All	All
Operating System	Linux	Linux Kernel	2.4.0	test1	All	All
Operating System	Linux	Linux Kernel	2.4.0	test10	All	All
Operating System	Linux	Linux Kernel	2.4.0	test11	All	All
Operating System	Linux	Linux Kernel	2.4.0	test12	All	All
Operating System	Linux	Linux Kernel	2.4.0	test2	All	All
Operating System	Linux	Linux Kernel	2.4.0	test3	All	All
Operating System	Linux	Linux Kernel	2.4.0	test4	All	All
Operating System	Linux	Linux Kernel	2.4.0	test5	All	All
Operating System	Linux	Linux Kernel	2.4.0	test6	All	All
Operating System	Linux	Linux Kernel	2.4.0	test7	All	All
Operating System	Linux	Linux Kernel	2.4.0	test8	All	All
Operating System	Linux	Linux Kernel	2.4.0	test9	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	2.4.18	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	2.4.19	All	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:2.4.0:*****:						
cpe:2.3:o:linux:linux_kernel:2.4.0:test1:*****:						
cpe:2.3:o:linux:linux_kernel:2.4.0:test10:*****:						
cpe:2.3:o:linux:linux_kernel:2.4.0:test11:*****:						
cpe:2.3:o:linux:linux_kernel:2.4.0:test12:*****:						
cpe:2.3:o:linux:linux_kernel:2.4.0:test2:*****:						
cpe:2.3:o:linux:linux_kernel:2.4.0:test3:*****:						
cpe:2.3:o:linux:linux_kernel:2.4.0:test4:*****:						
cpe:2.3:o:linux:linux_kernel:2.4.0:test5:*****:						
cpe:2.3:o:linux:linux_kernel:2.4.0:test6:*****:						
cpe:2.3:o:linux:linux_kernel:2.4.0:test7:*****:						
cpe:2.3:o:linux:linux_kernel:2.4.0:test8:*****:						
cpe:2.3:o:linux:linux_kernel:2.4.0:test9:*****:						
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:2.4.18: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:2.4.19:*.:*:*:*:*.*
```

```
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:2.4.0:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux kernel:2.4.0:test1:*:*:*:*:*:
```

cpe:2.3:o:linux:linux_kernel:2.4.0:test10:~::~~::~~::~~::~::
cpe:2.3:o:linux:linux_kernel:2.4.0:test11:~::~~::~~::~~::~::
cpe:2.3:o:linux:linux_kernel:2.4.0:test12:~::~~::~~::~~::~::
cpe:2.3:o:linux:linux_kernel:2.4.0:test2:~::~~::~~::~~::~::
cpe:2.3:o:linux:linux_kernel:2.4.0:test3:~::~~::~~::~~::~::
cpe:2.3:o:linux:linux_kernel:2.4.0:test4:~::~~::~~::~~::~::
cpe:2.3:o:linux:linux_kernel:2.4.0:test5:~::~~::~~::~~::~::
cpe:2.3:o:linux:linux_kernel:2.4.0:test6:~::~~::~~::~~::~::
cpe:2.3:o:linux:linux_kernel:2.4.0:test7:~::~~::~~::~~::~::
cpe:2.3:o:linux:linux_kernel:2.4.0:test8:~::~~::~~::~~::~::
cpe:2.3:o:linux:linux_kernel:2.4.0:test9:~::~~::~~::~~::~::
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:2.4.18: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:2.4.19:*****:
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