



CVE-2004-1056

Published on: 12/22/2004 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:09 PM UTC

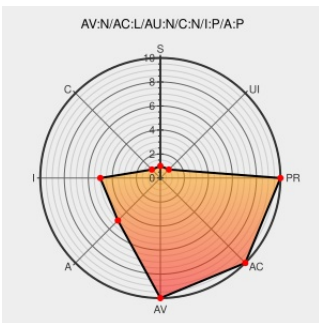
CVE-2004-1056

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

Direct Rendering Manager (DRM) driver in Linux kernel 2.6 does not properly check the DMA lock, which could allow remote attackers or local users to cause a denial of service (X Server crash) and possibly modify the video output.

CVE-2004-1056 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **6.4 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

[rhn.redhat.com](#) | Red Hat Support

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

[REDHAT RHSA-2005:663](#)

Webmail - OVH

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

[VUPEN ADV-2005-1878](#)

[usn/usn-38-1](#) - Ubuntu Linux

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

[UBUNTU USN-38-1](#)

[rhn.redhat.com](#) | Red Hat Support

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

[REDHAT RHSA-2005:529](#)

[rhn.redhat.com](#) | Red Hat Support

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

[REDHAT RHSA-2005:092](#)

No Description Provided

[bugzilla.fedora.us](#)

[FEDORA FLSA:2336](#)

Inactive Link Not Archived

Secunia - Advisories - Red Hat update for kernel

web.archive.org

text/html

SECUNIA 17002

rhn.redhat.com | Red Hat Support

www.redhat.com

text/html

REDHAT RHSA-2005:551

IBM X-Force Exchange

exchange.xforce.ibmcloud.com

text/html

XF linux-i810-dma-dos(15972)

Repository / Oval Repository

oval.cisecurity.org

text/html

OVAL oval:org.mitre.oval:def:9795

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	2.6.0	All	All	All
Operating System	Linux	Linux Kernel	2.6.0	test1	All	All
Operating System	Linux	Linux Kernel	2.6.0	test10	All	All
Operating System	Linux	Linux Kernel	2.6.0	test11	All	All
Operating System	Linux	Linux Kernel	2.6.0	test2	All	All
Operating System	Linux	Linux Kernel	2.6.0	test3	All	All
Operating System	Linux	Linux Kernel	2.6.0	test4	All	All
Operating System	Linux	Linux Kernel	2.6.0	test5	All	All
Operating System	Linux	Linux Kernel	2.6.0	test6	All	All
Operating System	Linux	Linux Kernel	2.6.0	test7	All	All
Operating System	Linux	Linux Kernel	2.6.0	test8	All	All
Operating System	Linux	Linux Kernel	2.6.0	test9	All	All
Operating System	Linux	Linux Kernel	2.6.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.1	rc1	All	All

Operating System	Linux	Linux Kernel	2.6.1	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.1	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.10	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.6	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.7	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.8	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.8	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.8	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.9	2.6.20	All	All
Operating System	Linux	Linux Kernel	2.6_test9_cvs	All	All	All
Operating System	Linux	Linux Kernel	2.6.0	All	All	All
Operating System	Linux	Linux Kernel	2.6.0	test1	All	All
Operating System	Linux	Linux Kernel	2.6.0	test10	All	All
Operating System	Linux	Linux Kernel	2.6.0	test11	All	All
Operating System	Linux	Linux Kernel	2.6.0	test2	All	All
Operating System	Linux	Linux Kernel	2.6.0	test3	All	All
Operating System	Linux	Linux Kernel	2.6.0	test4	All	All

Operating System	Linux	Linux Kernel	2.6.0	test4	All	All
Operating System	Linux	Linux Kernel	2.6.0	test5	All	All
Operating System	Linux	Linux Kernel	2.6.0	test6	All	All
Operating System	Linux	Linux Kernel	2.6.0	test7	All	All
Operating System	Linux	Linux Kernel	2.6.0	test8	All	All
Operating System	Linux	Linux Kernel	2.6.0	test9	All	All
Operating System	Linux	Linux Kernel	2.6.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.1	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.1	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.10	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.6	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.7	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.8	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.8	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.8	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.9	2.6.20	All	All
Operating System	Linux	Linux Kernel	2.6.10	All	All	All

Operating System	Linux	Linux Kernel	2.6_test9_cvs	All	All	All
Operating System	Ubuntu	Ubuntu Linux	4.1	All	ia64	All
Operating System	Ubuntu	Ubuntu Linux	4.1	All	ppc	All
Operating System	Ubuntu	Ubuntu Linux	4.1	All	ia64	All
Operating System	Ubuntu	Ubuntu Linux	4.1	All	ppc	All
cpe:2.3:o:linux:linux_kernel:2.6.0:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.0:test1:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.0:test10:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.0:test11:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.0:test2:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.0:test3:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.0:test4:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.0:test5:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.0:test6:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.0:test7:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.0:test8:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.0:test9:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.1:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.1:rc1:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.1:rc2:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.10:rc2:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.2:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.3:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.4:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.5:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.6:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.6:rc1:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.7:*:*:*:*:*:						

СРЕ.З.О.ИИИУХ.ИИИУХ_КЕИИЕ.З.О.Г

```
cpe:2.3:o:linux:linux_kernel:2.6.7:rc1:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.8:*:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.8:rc1:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.8:rc2:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.8.rc3:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.9:2.6.20:*:*:*:*:*:*
```

```
cpe:2.3:o:linux:linux_kernel:2.6_test9_cvs:*:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.0:*:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.0:test1:::*.*.*.*.*.*
```

```
cpe:2.3:o:linux:linux_kernel:2.6.0:test10:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.0:test11:::.*:.*:.*:.*
```

```
cpe:2.3:o:linux:linux_kernel:2.6.0:test2:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.0:test3:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.0:test4:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.0:test5:*:*:*:*:*
```

```
cpe:2.3:o:linux:linux_kernel:2.6.0:test6:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.0:test7:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.0:test8:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.1:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.1:rc1:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.1:rc2:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.10:rc2:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.2:*:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.3:*:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.4:*:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.5:*:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux kernel:2.6.6:*:*:*:*:*:
```

cpe:2.3:o:linux:linux_kernel:2.6.6:rc1:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.7:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.7:rc1:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.8:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.8:rc1:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.8:rc2:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.8:rc3:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.9:2.6.20:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6_test9_cvs:*:*:*:*:*:
cpe:2.3:o:ubuntu:ubuntu_linux:4.1:*:ia64:*:*:*:*:
cpe:2.3:o:ubuntu:ubuntu_linux:4.1:*:ppc:*:*:*:*:
cpe:2.3:o:ubuntu:ubuntu_linux:4.1:*:ia64:*:*:*:*:
cpe:2.3:o:ubuntu:ubuntu_linux:4.1:*:ppc:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)